

# Buchberger-Weispfenning Theory for Effective Associative Rings

**Michela Ceria**

Dipartimento di Ingegneria e scienza dell'informazione  
Università di Trento  
michela.ceria@unitn.it

**Teo Mora**

DIMA  
Università di Genova  
theomora@disi.unige.it

November 29, 2016

## Abstract

We present here a new approach for computing Gröbner bases for bilateral modules over an effective ring. Our method is based on Weispfenning notion of restricted Gröbner bases and related multiplication.

For (commutative) polynomial rings  $\mathbb{F}[X_1, \dots, X_n]$  [3, 4, 7, 5] over a field, Gröbner bases are computed by an iterative application of Buchberger test/completion which states that *a basis  $F$  is Gröbner if and only if each element in the set of all  $S$ -polynomials*

$$\left\{ S(f_{\alpha'}, f_{\alpha}) := \frac{\text{lcm}(\mathbf{M}(f_{\alpha}), \mathbf{M}(f_{\alpha'}))}{\mathbf{M}(f_{\alpha})} f_{\alpha} - \frac{\text{lcm}(\mathbf{M}(f_{\alpha}), \mathbf{M}(f_{\alpha'}))}{\mathbf{M}(f_{\alpha'})} f_{\alpha'} : f_{\alpha}, f_{\alpha'} \in F \right\}$$

*between two elements of  $F$ , reduces to 0.*

The same result holds for free monoid rings  $\mathbb{F}\langle X_1, \dots, X_n \rangle$  over a field, even if the shape of the *matches* (S-polynomials) between two elements is more involved and, in general, between two elements there could even be *infinitely many* S-polynomials; of course, in this setting, there is no hope of termination. Anyway, there are classical techniques [34] producing a procedure which, receiving as input a finite generating set  $F$  for the module  $\mathbb{I}(F)$ , provided that  $\mathbb{I}(F)$  has a finite Gröbner basis, halts returning such a finite Gröbner basis.

In both cases, it is well known that Buchberger test/completion is definitely superseded in each honest survey of Buchberger Theory and (what is more important) in all available implementations, by the test/completion based on the lifting theorem [22]: *a generating set  $F$  is a Gröbner basis if and only if each element in a minimal basis*

of the syzygies among the leading monomials  $\{\mathbf{M}(f_\alpha) : f_\alpha \in F\}$  lifts, via Buchberger reduction, to a syzygy among the elements of  $F$ .

The point is that the lifting theorem allowed Gebauer–Möller [11] to give more efficient criteria. Thus they detect at least as many “useless” pairs as Buchberger’s two criteria [5], but *they do not need to verify whether a pair satisfies the conditions required by the Second Criterion and thus they avoid the consequent bottleneck* needed for listing and ordering the S-pairs (in the commutative case they are  $(\#F)^2$  while a careful informal analysis in that setting suggests that the S-pairs needed by Gebauer–Möller Criterion are  $n\#F$ ). Moreover, the flexibility of Möller lifting theorem approach - with respect to Buchberger S-pair test - allows the former to extend Buchberger theory *verbatim* at least to (non commutative) monoid rings over PIRs.

We can remark that Buchberger Theory and Algorithm for left (or right) ideals of monoid rings over PIRs essentially repeats *verbatim* the same Theory and Algorithm as the commutative case.

The same happens in the first class of twisted polynomial rings whose Buchberger Theory and Algorithm has been studied, *solvable polynomial rings* over a field [15]: there the left case is obtained simply by reformulating Buchberger test, while the bilateral case is solved via Kandri-Rody—Weispfenning completion which essentially consists of a direct application of Spear’s Theorem.

Later, Weispfenning studied an interesting class of rings,  $\mathbb{Q}\langle x, Y \rangle / \mathbb{I}(Yx - x^e Y)$ ,  $e \in \mathbb{N}, e > 1$  [44], [26, IV.49.11, IV.50.13.6], and essentially applied the same kind of completion: instead of the bilateral ideal

$$\mathbb{I}_2 := \text{Span}_{\mathbb{Q}}(x^a Y^b f x^c Y^d : (a, b, c, d) \in \mathbb{N}^4)$$

he considered the *restricted* ideal

$$\mathbb{I}_W := \text{Span}_{\mathbb{Q}}(x^a f Y^d : (a, d) \in \mathbb{N}^2).$$

Then he computed a *restricted Gröbner basis* of it via Buchberger test and extended this restricted Gröbner basis to the required bilateral Gröbner basis via a direct application of Spear’s Theorem. The point is that, if we denote  $\diamond$  the commutative multiplication

$$x^a Y^d \diamond x^c Y^b = x^{a+c} Y^{b+d}, (a, b, c, d) \in \mathbb{N}^4,$$

the computation of restricted Gröbner bases *verbatim* mimicks the commutative case as it was done for left ideals in the case of solvable polynomial rings.

A Buchberger Theory for each effective ring

$$\mathcal{A} = \mathcal{Q}/I, \mathcal{Q} := \mathbb{D}\langle \overline{\mathbf{v}} \sqcup \overline{\mathbf{V}} \rangle, I = \mathbb{I}_2(G),$$

where  $\mathbb{D}$  is a PID and  $G$  a Gröbner basis w.r.t. a suitable term ordering  $<$ , has been recently proposed in [26, IV.50] (for an abridged survey see [23]), using the strength of Möller lifting theorem.

In this setting, denoting  $G_0 := G \cap \mathbb{D}\langle \overline{\mathbf{v}} \rangle$ , we need to consider S-pairs among elements which essentially have the shape

$$- a\omega f, f \in F, \omega \in \langle \overline{\mathbf{v}} \rangle, a \in \mathbb{D}\langle \overline{\mathbf{v}} \rangle / \mathbb{I}_2(G_0) \text{ in the left case, and}$$

–  $a\lambda fb\rho, f \in F, \lambda, \rho \in \langle \bar{\mathbf{V}} \rangle, a, b \in \mathbb{D}\langle \bar{\mathbf{V}} \rangle / \mathbb{I}_2(G_0)$  in the bilateral case.

While reading the proofs of [26, IV] the senior author realized a wrong description of the S-polynomials required by the bilateral lifting theorem in an example involving the Ore algebra  $\mathbb{Z}[X, Y, Z] / \mathbb{I}(YX - 2XY, ZX - 3XZ, ZY - 5XZ)$  [26, IV.50.11.8] which was therefore forced to remove; at the same time, however, the reading of the section devoted to Weispfenning ring suggested him how to formalize an intuition informally expressed in [25]. Applying this approach to Ore algebras [9] the junior author formalized the notion of Weispfenning multiplication  $\diamond$  and realized that it allows to extend *verbatim* Buchberger First Criterion and, consequently, the algorithms based on Gebauer-Möller Criteria [11], [26, II.25.1].

This provides an alternative (and more efficient) approach for producing bilateral Gröbner bases, via the notion of restricted Gröbner bases, for which we have to apply the test to elements having the shape

–  $a\omega \diamond f, f \in F, \omega \in \langle \bar{\mathbf{V}} \rangle, a \in \mathbb{D}\langle \bar{\mathbf{V}} \rangle / \mathbb{I}_2(G_0)$

and for which Gebauer-Möller Criteria are available; once a bilateral Gröbner basis is thus produced a direct application of Spear Theorem is all one needs.

In Sections 1-3 we discuss in detail our notion of *effective ring*, i.e. a ring  $\mathcal{A}$  presented, accordingly the universal property of free monoid rings, as a quotient  $\mathcal{A} = Q/I$  of a free monoid ring  $Q := \mathbb{D}\langle \bar{\mathbf{V}} \sqcup \bar{\mathbf{V}} \rangle$  modulo a bilateral ideal  $I = \mathbb{I}_2(G)$ , presented in turn by its Gröbner basis w.r.t. a suitable term ordering  $<$ . Thus the ring  $\mathcal{A}$  turns out to be a left R-module over the effectively given ring

$$R := \mathcal{R} / \mathbb{I}_2(G_0), \mathcal{R} := \mathbb{D}\langle \bar{\mathbf{V}} \rangle, G_0 := G \cap \mathcal{R}.$$

In Section 4 we discuss the pseudovaluation [1] which is naturally induced on  $\mathcal{A}$  by the classical filtration/valuation of  $Q$  related with Buchberger Theory, so that in Section 5 we can import on  $\mathcal{A}$  the notions and main properties of Gröbner bases, Gröbner presentation, normal forms.

At the same time after having introduced Weispfenning multiplication (Section 6), we can extend the same notions and properties (Section 7) to the case of restricted modules, proving a lifting theorem for them (Section 8) and consequently listing the S-polynomials needed to test/completing a restricted basis (Section 11); an adaptation of Weispfenning Completion in this setting (Section 9), allows to produce, iteratively, a bilateral Gröbner basis from which a strong bilateral Gröbner basis can be easily deduced (Section 12).

Of course, in this setting it is well-known that there is no chance to hope for a terminating algorithm, unless the ring is noetherian and its representation is properly restricted; the classical approach consists in producing a procedure which terminates if and only if the module generated by a given finite basis has a finite Gröbner basis which, in this case, is returned (Section 10).

The paper is completely self-contained and can be read without knowing [26] and [23]; it requires however a good knowledge of the classical papers on which is based the

core of Buchberger Theory: the results by Buchberger [3, 4, 7, 5], Spear [40], Zacharias [47], Möller [22], Gebauer-Möller [11], Traverso [43, 12], Weispfenning [15, 2, 44], Pritchard [33, 34], Apel [1].

## 1 Effectiveness

Given any set  $\bar{\mathbb{Z}}$  and denoting  $\langle \bar{\mathbb{Z}} \rangle$  the monoid of all words over the alphabet  $\bar{\mathbb{Z}}$ , we can consider the free monoid ring  $\mathbb{Q} := \mathbb{D}\langle \bar{\mathbb{Z}} \rangle$  of  $\langle \bar{\mathbb{Z}} \rangle$  over the principal ideal domain  $\mathbb{D}$  whose elements are the finite sums of “monomials”  $c\tau$ ,  $c \in \mathbb{D}$ ,  $\tau \in \langle \bar{\mathbb{Z}} \rangle$ , and whose product is obtained by distributing the word concatenation of  $\langle \bar{\mathbb{Z}} \rangle$ :

$$cx_1x_2 \dots x_m \cdot dy_1 \dots y_n = cdx_1x_2 \dots x_my_1 \dots y_n \text{ for each } c, d \in \mathbb{D}, x_i, y_j \in \bar{\mathbb{Z}}.$$

The ring  $\mathbb{Q} := \mathbb{Z}\langle \bar{\mathbb{Z}} \rangle$  has the following universal property: any map  $\bar{\mathbb{Z}} \rightarrow A$  over any ring with identity  $A$  can be uniquely extended to a ring morphism  $\mathbb{Q} \rightarrow A$ . Therefore:

**Fact 1.** *For a (not necessarily commutative) ring with identity  $A$ , there is a (not necessarily finite nor necessarily countable) set  $\bar{\mathbb{Z}}$  and a projection  $\Pi : \mathbb{Q} := \mathbb{Z}\langle \bar{\mathbb{Z}} \rangle \twoheadrightarrow A$  so that, denoting  $\mathfrak{l} \subset \mathbb{Q} = \mathbb{Z}\langle \bar{\mathbb{Z}} \rangle$  the bilateral ideal  $\mathfrak{l} := \ker(\Pi)$ , we have  $A = \mathbb{Q}/\mathfrak{l}$ .*

*Proof.* It is sufficient to consider the set  $\bar{\mathbb{Z}} := A$  and the identity map  $\bar{\mathbb{Z}} := A \rightarrow A$  in order to obtain the result by the universal property of  $\mathbb{Q} := \mathbb{Z}\langle A \rangle$ .  $\square$

Of course, each *commutative* ring  $A$  can be represented in a similar way as a quotient of the commutative polynomial ring  $\mathbb{P} := \mathbb{Z}[\bar{\mathbb{Z}}]$  modulo an ideal  $\mathfrak{l}$ .

Let  $R$  be a (not necessarily commutative) ring with identity  $\mathbf{1}_R$  and  $\mathcal{A}$  another (not necessarily commutative) ring with identity  $\mathbf{1}_{\mathcal{A}}$  which is a left module on  $R$ .

**Definition 2.** [27] We consider  $\mathcal{A}$  to be *effectively given* when we are given

- a Zacharias [26, II.26.1] principal ideal domain  $\mathbb{D}$  with *canonical representatives* [27];
- sets  $\bar{\mathbf{v}} := \{x_1, \dots, x_j, \dots\}$ ,  $\bar{\mathbf{v}} := \{X_1, \dots, X_i, \dots\}$ , which are *countable*, and
- $\bar{\mathbb{Z}} := \bar{\mathbf{v}} \sqcup \bar{\mathbf{v}} = \{x_1, \dots, x_j, \dots, X_1, \dots, X_i, \dots\}$ ;
- rings  $\mathcal{R} := \mathbb{D}\langle \bar{\mathbf{v}} \rangle \subset \mathbb{Q} := \mathbb{D}\langle \bar{\mathbb{Z}} \rangle$ ;
- projections  $\pi : \mathcal{R} = \mathbb{D}\langle x_1, \dots, x_j, \dots \rangle \twoheadrightarrow R$  and
- $\Pi : \mathbb{Q} := \mathbb{D}\langle x_1, \dots, x_j, \dots, X_1, \dots, X_i, \dots \rangle \twoheadrightarrow \mathcal{A}$  which satisfy

$$\Pi(x_j) = \pi(x_j)\mathbf{1}_{\mathcal{A}}, \text{ for each } x_j \in \bar{\mathbf{v}},$$

so that  $\Pi(\mathcal{R}) = \{r\mathbf{1}_{\mathcal{A}} : r \in R\} \subset \mathcal{A}$ .

Thus denoting

- $\mathcal{I} := \ker(\Pi) \subset \mathcal{Q}$  and
- $\mathcal{I} := \mathcal{I} \cap \mathcal{R} = \ker(\pi) \subset \mathcal{R}$ ,

we have  $\mathcal{A} = \mathcal{Q}/\mathcal{I}$  and  $R = \mathcal{R}/\mathcal{I}$ ; moreover we can wlog assume that  $R \subset \mathcal{A}$ .

Further, when considering  $\mathcal{A}$  as effectively given in this way, we explicitly impose the Ore-like requirement that

$$X_i x_j \equiv \sum_{l=1}^i \pi(a_{lij}) X_l + \pi(a_{0ij}) \bmod \mathcal{I}, a_{lij} \in \mathbb{D}(\overline{\mathbf{v}}), \quad (1)$$

for all  $X_i \in \overline{\mathbf{V}}, x_j \in \overline{\mathbf{v}}$ .

*Remark 3.*

1. It is sufficient to consider the uncountable field of the reals  $\mathbb{R}$ , to understand that not necessarily each ring  $\mathcal{A}$  can be provided of a Buchberger Theory.

Essentially, our definition of an *effectively given* ring  $\mathcal{A}$  is a specialization of the one introduced (under the same name of *explizite-bekannt*) for fields by van der Waerden [46]; the difference is that the ability of performing arithmetics in *endlichvielen Schritten* is granted here by the implicit assumption of knowing a Gröbner basis of  $\mathcal{I}$ .

Moreover, in the commutative case, the recent result of [45] which, following an old idea of Buchberger [6], obtains a degree-bound evaluation for ideal membership test and canonical form computation by merging Grete Hermann's [14] and Dubé's [10] bounds, grants a representation of  $\mathcal{A}$  which even satisfies Hermann's [14, p.736] requirement of *an upper bound for the number of operations needed by the computation*.

If we are interested in polynomial rings with coefficients in  $\mathbb{R}$  or in a ring of analytical functions (as in Riquiet-Janet Theory [17, 18, 32]), since a given finite basis has a finite number of coefficients  $c_i \in R$ , the requirement that the data are effectively given essentially means that we need to provide the algebraically dependencies among such  $c_i$ .

For instance while the rings  $\mathbb{Q}[\pi]$  and  $\mathbb{Q}[e]$  can be considered effectively given as  $\mathbb{Q}[v]$  within Kronecker's Model [26, I.8.1-3.], the problem arises with  $\mathbb{Q}[\pi, e]$ : the Kronecker's Model  $\mathbb{Q}[v_1, v_2]$  is valid provided that  $\pi$  and  $e$  are algebraically independent; potential algebraic dependencies generate an ideal  $\mathcal{I} \subset \mathbb{Q}[v_1, v_2]$  and the ring can be considered effectively given under Definition 2 only if such ideal is explicitly produced thus representing  $\mathbb{Q}[\pi, e]$  as  $\mathbb{Q}[v_1, v_2]/\mathcal{I}$ ; the point, of course, is that the status of algebraically dependency between  $\pi$  and  $e$  is still open.

2. The Ore-like requirement (1), which wants that no higher-indexed "variable"  $X_l, l > i$ , appears in the representation, in the left  $\mathcal{R}$ -module  $\mathcal{A}$ , of a multiplication of a "variable"  $X_i$  at the right by a "coefficient"  $x_j$ , is necessary in order to avoid non-noetherian reductions.

In order to illustrate the rôle of condition (1), the most natural example is the free monoid ring  $\mathbb{Z}\langle x, y \rangle$  which is naturally a left  $\mathbb{Z}[x]$ -module; a natural choice for the generating set  $\langle \Pi(\bar{\mathbf{V}}) \rangle = \Pi(\langle \bar{\mathbf{V}} \rangle)$  is  $\bar{\mathbf{V}} = \{X_i, i \in \mathbb{N}\}$ ,  $\Pi(X_i) = yx^i$  which gives, through the isomorphism  $\Pi$ , the equivalent representation  $\mathbb{Z}\langle x, y \rangle \cong \mathbb{Z}[x]\langle \bar{\mathbf{V}} \rangle$  and the projection

$$\Pi : \mathbb{Z}\langle x, X_0, X_1, \dots \rangle \twoheadrightarrow \mathbb{Z}\langle x, y \rangle, \ker(\Pi) = \{X_i x - X_{i+1}, i \in \mathbb{N}\},$$

and in order to obtain  $\mathbf{T}(X_i x - X_{i+1}) = X_i x$  we are forced to use the non-noetherian ordering  $X_1 >_V X_2 >_V \dots >_V X_i >_V \dots$  on  $\bar{\mathbf{V}}$  which would require a related Hironaka Theory [13].

Thus our definition considers  $\mathbb{Z}\langle x, y \rangle$  as *not* effectively given as a left  $\mathbb{Z}[x]$ -module.  $\square$

For each  $m \in \mathbb{N}$ , we denote  $\{\mathbf{e}_1, \dots, \mathbf{e}_m\}$  the canonical basis of the free  $\mathcal{Q}$ -module  $\mathcal{Q}^m$ , whose basis as a left  $\mathbb{D}$ -module is the set of *terms*

$$\langle \bar{\mathbf{Z}} \rangle^{(m)} := \{t\mathbf{e}_i : t \in \langle \bar{\mathbf{Z}} \rangle, 1 \leq i \leq m\}.$$

If we impose on  $\langle \bar{\mathbf{Z}} \rangle^{(m)}$  a term ordering  $<$ , then each  $f \in \mathcal{Q}^m$  has a unique representation as an ordered linear combination of terms  $t \in \langle \bar{\mathbf{Z}} \rangle^{(m)}$  with coefficients in  $\mathbb{D}$ :

$$f = \sum_{i=1}^s c(f, t_i) t_i : c(f, t_i) \in \mathbb{D} \setminus \{0\}, t_i \in \langle \bar{\mathbf{Z}} \rangle^{(m)}, t_1 > \dots > t_s.$$

The *support* of  $f$  is the set  $\text{supp}(f) := \{t : c(f, t) \neq 0\}$ ; we further denote  $\mathbf{T}(f) := t_1$  the *maximal term* of  $f$ ,  $\text{lc}(f) := c(f, t_1)$  its *leading coefficient* and  $\mathbf{M}(f) := c(f, t_1)t_1$  its *maximal monomial*.

For a subset  $G \subset \mathcal{Q}^m$  of a module  $\mathcal{Q}^m$ ,  $\mathbb{I}_L(G), \mathbb{I}_R(G), \mathbb{I}_2(G)$  denotes the left (resp. right, bilateral) module generated by  $G$ , the index being dropped when there is no need of specification; moreover  $\mathbf{T}\{G\}$  denotes the set

$$\mathbf{T}\{G\} := \{\mathbf{T}(f) : f \in G\} \subset \langle \bar{\mathbf{Z}} \rangle^{(m)}.$$

## 2 Recalls on Zacharias rings and canonical representation

Zacharias approach [47] to Buchberger Theory consisted in remarking that, if each module  $\mathbf{l} \subset R\langle \bar{\mathbf{Z}} \rangle^m$  has a groebnerian property, necessarily the same property must be satisfied at least by the modules  $\mathbf{l} \subset R^m \subset R\langle \bar{\mathbf{Z}} \rangle^m$  and thus such property in  $R$  is available and can be used to devise a procedure granting the same property in  $R\langle \bar{\mathbf{Z}} \rangle^m$ . The most elementary applications of Zacharias approach is the generalization (up to membership test and syzygy computation) of the property of canonical forms from the case in which  $R = \mathbb{F}$  is a field to the general case: all we need is an effective notion of canonical forms for modules in  $R$ .

**Definition 4** (Zacharias). [47] A ring  $R$  is said to have *canonical representatives* if there is an algorithm which, given an element  $c \in R^m$  and a (left, bilateral, right) module  $J \subset R^m$ , computes a *unique* element  $\mathbf{Rep}(c, J) \in R^m$  such that

- $c - \mathbf{Rep}(c, J) \in J$ ,
- $\mathbf{Rep}(c, J) = 0 \iff c \in J$ .

The set

$$R^m \supset \mathbf{Zach}(R^m/J) := \mathbf{Rep}(J) := \{\mathbf{Rep}(c, J) : c \in R^m\} \cong R^m/J$$

is called the *canonical Zacharias representation* of the module  $R^m/J$ .  $\square$

Remark that, for each  $c, d \in R^m$  and each module  $J \subset R^m$ , we have

$$c - d \in J \iff \mathbf{Rep}(c, J) = \mathbf{Rep}(d, J).$$

**Definition 5.** [47] (cf. [26, II. Definition 26.1.1]) A ring  $R$  with identity is called a (left) *Zacharias ring* if it satisfies the following properties:

- (a).  $R$  is a noetherian ring;
- (b). there is an algorithm which, for each  $c \in R^m$ ,  $C := \{c_1, \dots, c_t\} \subset R^m \setminus \{0\}$ , allows to decide whether  $c \in \mathbb{I}_L(C)$  in which case it produces elements  $d_i \in R : c = \sum_{i=1}^t d_i c_i$ ;
- (c). there is an algorithm which, given  $\{c_1, \dots, c_t\} \subset R^m \setminus \{0\}$ , computes a finite set of generators for the left syzygy  $R$ -module  $\{(d_1, \dots, d_t) \in R^t : \sum_{i=1}^t d_i c_i = 0\}$ .

Note that [22] for a ring  $R$  with identity which satisfies (a) and (b), (c) is equivalent to

- (d). there is an algorithm which, given  $\{c_1, \dots, c_s\} \subset R^m \setminus \{0\}$ , computes a finite basis of the ideal

$$\mathbb{I}_L(\{c_i : 1 \leq i < s\}) : \mathbb{I}_L(c_s).$$

If  $R$  has canonical representatives, we improve the computational assumptions of Zacharias rings, requiring also the following property:

- (e). there is an algorithm which, given an element  $c \in R^m$  and a left module  $J \subset R^m$ , computes the unique canonical representative  $\mathbf{Rep}(c, J)$ .  $\square$

We can now precise our assumption on  $\mathbb{D}$  requiring that it is a Zacharias PID with canonical representatives.

We begin by noting that when  $\mathbb{D} = \mathbb{Z}$ , for each  $m \in \mathbb{Z}$ , reasonable sets  $A_m$  of the canonical representatives of the residue classes of  $\mathbb{Z}_m = \mathbb{Z}/\mathbb{I}(m)$  are

$$A_m = \{z \in \mathbb{Z} : -\frac{m}{2} < z \leq \frac{m}{2}\}, A_m = \{z \in \mathbb{Z} : 0 < z \leq m\} \text{ or } A_m = \{z \in \mathbb{Z} : 0 \leq z < m\}.$$

In the general case we remark that, if we use Szekeres notation [42], [26, IV.46.1.1.2], [27] and denote  $\mathbb{I}_\tau$  the left *Szekeres ideal*

$$\mathbb{I}_\tau := \{\mathbb{I}c(f) : f \in \mathbb{I}, \mathbf{T}(f) = \tau\} \cup \{0\} = \mathbb{I}(c_\tau) \subset \mathbb{D}$$

and  $c_\tau$  its *Szekeres generator*, for each module  $\mathbb{I} \subset \mathcal{Q}^m$  and each  $\tau \in \langle \overline{\mathbb{Z}} \rangle^{(m)}$ , we obtain

- the relation

$$\omega \mid \tau \implies c_\tau \mid c_\omega,$$

for each  $\tau, \omega \in \mathbf{T}\{\mathbf{l}\} := \{\mathbf{T}(f) : f \in \mathbf{l}\} \subset \langle \overline{\mathbf{Z}} \rangle^{(m)}$ ;

- the partition  $\langle \overline{\mathbf{Z}} \rangle^{(m)} = \mathbf{L}(\mathbf{l}) \sqcup \mathbf{R}(\mathbf{l}) \sqcup \mathbf{N}(\mathbf{l})$  of  $\langle \overline{\mathbf{Z}} \rangle^{(m)}$  where

- $\mathbf{N}(\mathbf{l}) := \{\tau \in \langle \overline{\mathbf{Z}} \rangle^{(m)} : \mathbf{l}_\tau = (0)\}$ ,
- $\mathbf{L}(\mathbf{l}) := \{\tau \in \langle \overline{\mathbf{Z}} \rangle^{(m)} : \mathbf{l}_\tau = \mathbb{D}\}$ ,
- $\mathbf{R}(\mathbf{l}) := \{\tau \in \langle \overline{\mathbf{Z}} \rangle^{(m)} : \mathbf{l}_\tau \notin \{(0), \mathbb{D}\}\}$ ;

- the *canonical Zacharias representation*

$$\begin{aligned} Q^m \supset \mathbf{Zach}(Q^m/\mathbf{l}) := \mathbf{Rep}(\mathbf{l}) &= \left\{ \mathbf{Rep}(c, \mathbf{l}) : c \in Q^m \right\} \\ &:= \bigoplus_{\tau \in \langle \overline{\mathbf{Z}} \rangle^{(m)}} \mathbf{Rep}(\mathbf{l}_\tau) \tau \\ &= \bigoplus_{\tau \in \mathcal{T}^{(m)}} \mathbf{Zach}(R/\mathbf{l}_\tau) \tau \cong Q^m/\mathbf{l} \end{aligned}$$

of the module  $Q^m/\mathbf{l}$ .

### 3 Zacharias canonical representation of Effective Associative Rings

If we fix

- a term-ordering  $<$  on  $\langle \overline{\mathbf{Z}} \rangle$

we can assume  $\mathcal{I}$  to be given via

- its bilateral Gröbner basis  $G$  w.r.t.  $<$

and, if  $<$  satisfies

$$X_i > t \text{ for each } t \in \overline{\mathbf{v}} \text{ and } X_i \in \overline{\mathbf{v}}, \quad (2)$$

also  $\mathcal{I}$  is given via

- its bilateral Gröbner basis  $G_0 := G \cap \mathcal{R}$  w.r.t.  $<$ .

Since condition (1) implies that, for each  $X_i \in \overline{\mathbf{v}}, x_j \in \overline{\mathbf{v}}$ ,

$$f_{ij} := X_i x_j - \sum_{l=1}^i a_{lij} X_l - a_{0ij} \in \mathcal{I} \subset Q,$$

if we further require that  $<$  satisfies

$$X_i x_j = \mathbf{T}(f_{ij}) \text{ for each } X_i \in \overline{\mathbf{v}}, x_j \in \overline{\mathbf{v}}, \quad (3)$$

and denote  $C := \{f_{ij} : X_i \in \overline{\mathbf{v}}, x_j \in \overline{\mathbf{v}}\}$  we have



- $G_0 \sqcup C \subset G$ ,
- $\mathcal{A}$  is generated as  $R$ -module by  $\Pi(\langle \bar{\mathbf{V}} \rangle)$  and,
- as  $\mathbb{D}$ -module, by a subset of  $\{\nu\omega : \nu \in \langle \bar{\mathbf{V}} \rangle, \omega \in \langle \bar{\mathbf{V}} \rangle\}$ .

Thus, using Szekeres notation and setting  $A_{c_\tau} := \mathbb{D}/I_\tau$  for each  $\tau \in \langle \bar{\mathbf{Z}} \rangle$ ,  $\mathcal{A}$  can be described via its Zacharias canonical representation w.r.t.  $<$  as

$$\mathcal{A} = Q/I \cong \bigoplus_{\omega \in \langle \bar{\mathbf{V}} \rangle} \left( \bigoplus_{\nu \in \langle \bar{\mathbf{V}} \rangle} A_{c_{\nu\omega}} \nu \right) \omega =: \mathbf{Zach}_{<}(\mathcal{A}) \subset Q. \quad (4)$$

*Example 6.* W.r.t. the ideal  $\mathfrak{l} := \mathbb{I}(2X, 3Y) \in \mathbb{Z}[X, Y]$  whose strong Gröbner basis is  $\{2X, 3Y, XY\}$ , the ring

$$\mathcal{A} := \mathbb{Z}[X, Y]/\mathfrak{l} \cong \mathbb{Z}\langle X, Y \rangle / \mathbb{I}_2(2X, 3Y, XY, YX)$$

has the canonical representation

$$\mathcal{A} \cong \mathbb{Z} + \mathbb{Z}_2[X]X + \mathbb{Z}_3[Y]Y;$$

thus the underlying  $\mathbb{Z}$ -module has the structure

$$\mathcal{A} \cong \mathbb{Z} \oplus \left( \bigoplus_{i \in \mathbb{N} \setminus \{0\}} \mathbb{Z}_2 \right) \oplus \left( \bigoplus_{i \in \mathbb{N} \setminus \{0\}} \mathbb{Z}_3 \right)$$

and the ring structure is defined by

$$(a, \dots, d_i, \dots, g_i, \dots) \star (b, \dots, e_i, \dots, h_i, \dots) = (c, \dots, f_i, \dots, l_i, \dots)$$

where  $a, b, c \in \mathbb{Z}, d_i, e_i, f_i \in \mathbb{Z}_2 \cong \{0, 1\}, g_i, h_i, l_i \in \mathbb{Z}_3 \cong \{-1, 0, 1\}$  and

$$\begin{aligned} c &:= ab, \\ f_i &:= \pi_2(a)e_i + \sum_{j=1}^{i-1} d_j e_{i-j} + d_i \pi_2(b), i \in \mathbb{N} \setminus \{0\}, \\ l_i &:= \pi_3(a)h_i + \sum_{j=1}^{i-1} g_j h_{i-j} + g_i \pi_3(b), i \in \mathbb{N} \setminus \{0\}. \end{aligned}$$

□

If we further consider, for each  $\omega \in \langle \bar{\mathbf{V}} \rangle$ , the left Szekeres ideal

$$I_\omega := \{r \in \mathcal{R} : \exists h \in Q, \mathbf{T}(h) < \omega, r\omega + h \in I\} \supset I = I \cap \mathcal{R}$$

and the ring  $R_\omega = \mathcal{R}/I_\omega$ , having the Zacharias canonical representation

$$\mathbf{Zach}_{<}(R_\omega) \cong \bigoplus_{\nu \in \langle \bar{\mathbf{V}} \rangle} A_{c_{\nu\omega}} \nu \subset \mathcal{R}$$

we obtain

$$\mathbf{Zach}_{<}(\mathcal{R}/\mathcal{I}_\omega) \subset \mathbf{Zach}_{<}(\mathcal{R}/I) = \mathbf{Zach}_{<}(R) \subset \mathcal{R}$$

and

$$\mathcal{A} \cong \bigoplus_{\omega \in \langle \bar{\mathbf{V}} \rangle} \left( \bigoplus_{v \in \langle \bar{\mathbf{V}} \rangle} A_{c_{v\omega}} v \right) \omega \cong \bigoplus_{\omega \in \langle \bar{\mathbf{V}} \rangle} R_\omega \omega \subset \mathcal{R}\langle \bar{\mathbf{V}} \rangle = \mathcal{Q}. \quad (5)$$

More precisely, denoting

- $\mathbf{N}(I) := \{\omega \in \langle \bar{\mathbf{V}} \rangle : I_\omega = I\},$
- $\mathbf{L}(I) := \{\omega \in \langle \bar{\mathbf{V}} \rangle : I_\omega = R\},$
- $\mathbf{R}(I) := \{\omega \in \langle \bar{\mathbf{V}} \rangle : I_\omega \notin \{I, R\}\}$

we have the partition  $\langle \bar{\mathbf{V}} \rangle = \mathbf{L}(I) \sqcup \mathbf{R}(I) \sqcup \mathbf{N}(I)$  and, denoting

$$\mathcal{B} = \mathbf{R}(I) \sqcup \mathbf{N}(I) = \langle \bar{\mathbf{V}} \rangle \setminus \mathbf{L}(I) \subset \langle \bar{\mathbf{V}} \rangle,$$

we obtain

1.  $\mathcal{B} \subset \langle \bar{\mathbf{V}} \rangle$  is an order module i.e.  $\lambda\tau\rho \in \mathcal{B} \implies \tau \in \mathcal{B}$  for each  $\lambda, \tau, \rho \in \langle \bar{\mathbf{V}} \rangle$ ;
2.  $\mathcal{A}$  is both a left  $\mathcal{R}$ -module and a left  $R$ -module with generating set  $\mathcal{B}$ .

Thus, each element  $f \in \mathcal{A}$  is uniquely represented via its canonical representation w.r.t.  $<$

$$\mathbf{Rep}(f, \mathcal{I}) = \sum_{\omega \in \mathcal{B}} a_\omega \omega \in \mathbf{Zach}_{<}(\mathcal{A})$$

where, using the present notation, each

$$a_\omega = \sum_{v \in \langle \bar{\mathbf{V}} \rangle} b_{v\omega} v \in \mathbf{Zach}_{<}(R_\omega)$$

is the canonical representation of an element of the module  $\mathcal{R}/\mathcal{I}_\omega$  and each  $b_{v\omega} \in A_{c_{v\omega}}$  is the canonical representation of an element of the ring  $A_{c_{v\omega}} := \mathbb{D}/\mathbb{I}(c_{v\omega}) = \mathbb{D}/\mathbb{I}_{v\omega}$ ; we will identify the elements in  $\mathcal{A}$ ,  $R_\omega$  and  $A_{c_{v\omega}}$  with their representatives.

*Example 7.* For  $\mathcal{Q} = \mathbb{Z}\langle x_1, x_2, X_1 \rangle$ ,

$$G_0 = \{x_2x_1\}, C = \{X_1x_1 - x_2X_1, X_1x_2 - x_1X_1\}, I = \mathbb{I}_2(G_0 \cup C), \mathcal{A} = \mathcal{Q}/I,$$

a minimal Gröbner basis of  $I$  is  $G_0 \cup C \cup \{x_1x_2^{i+1}X_1, i \in \mathbb{N}\}$ , since we have

$$x_1x_2X_1 = X_1 \star x_2x_1 - (X_1x_2 - x_1X_1) \star x_1 - x_1 \star (X_1x_1 - x_2X_1)$$

and, for  $i \geq 1$

$$x_1x_2^{i+1}X_1 = x_1x_2^iX_1 \star x_1 - x_1x_2^i \star (X_1x_1 - x_2X_1).$$

We therefore have

$$R = \mathbb{Z}\langle x_1, x_2 \rangle / \mathbb{I}(x_2x_1), \mathbf{Zach}_{<}(R) = \text{Span}_{\mathbb{Z}}\{x_1^i x_2^j : (i, j) \in \mathbb{N}^2\},$$

and, denoting  $R_l := R_{X_1^l}$ ,  $\mathcal{I}_l := \mathcal{I}_{X_1^l}$  for each  $l$ , we have, for  $l \geq 1$ ,

$$\mathcal{I}_l = \mathbb{I}_L(x_2 x_1, x_1 x_2^{i+1}, i \in \mathbb{N}), R_l = \mathbb{Z}\langle x_1, x_2 \rangle / \mathcal{I}_l \cong \mathbb{Z}[x_1, x_2] / \mathbb{I}(x_1 x_2)$$

so that  $\mathbf{Zach}_{<}(R_l) = \text{Span}_{\mathbb{Z}}\{x_1^i, x_2^j : i, j \in \mathbb{N}\}$  and

$$\mathbf{Zach}_{<}(\mathcal{A}) = \mathbb{Z}[x_1, x_2] \bigoplus \left( \bigoplus_{l \geq 1} \mathbb{Z}[x_1, x_2] / \mathbb{I}(x_1 x_2) X_1^l \right)$$

so that a generic element of  $\mathbf{Zach}_{<}(\mathcal{A})$  has the form

$$f(x_1, x_2) = a(x_1, x_2) + \sum_{l > 0} (b_l + c_l(x_1) + d_l(x_2)) X_1^l$$

with  $a \in \mathbb{Z}[x_1, x_2]$ ,  $b_l \in \mathbb{Z}$ ,  $c_l \in \mathbb{Z}[x_1]$ ,  $d_l \in \mathbb{Z}[x_2]$ ,  $c_l(0) = d_l(0) = 0$  and the related left  $R$ -algebra structure is defined by

$$\begin{aligned} x_1^{i+1} f(x_1, x_2) &= x_1^{i+1} a(x_1, x_2) + \sum_{l > 0} (b_l x_1^{i+1} + c_l(x_1) x_1^{i+1}) X_1^l, \\ x_2^{j+1} f(x_1, x_2) &= x_2^{j+1} a(0, x_2) + \sum_{l > 0} (b_l x_2^{j+1} + d_l(x_2) x_2^{j+1}) X_1^l, \\ x_1^{i+1} x_2^{j+1} f(x_1, x_2) &= x_1^{i+1} x_2^{j+1} a(0, x_2). \end{aligned}$$

□

*Remark 8.*

1. We must stress that all inclusions —  $A_{c_{\text{ew}}} \subset \mathbb{D}$ ,  $\mathbf{Zach}_{<}(R_{\omega}) \subset \mathcal{R} = \mathbb{D}\langle \overline{\mathbf{v}} \rangle$ ,  $\mathbf{Zach}_{<}(\mathcal{A}) \subset \mathcal{R}[\mathcal{B}] \subset \mathcal{R}\langle \overline{\mathbf{v}} \rangle$  — must be understood as *set* inclusions only and do not preserve the module structure and the notation  $\mathcal{R}\langle \overline{\mathbf{v}} \rangle$  does not denote the canonical monoid ring but, as the notation  $\mathcal{R}[\mathcal{B}]$ , only the underlying free left  $\mathcal{R}$ -modules with bases  $\langle \overline{\mathbf{v}} \rangle$  and  $\mathcal{B}$ .
2. Note that Zacharias' approach holds for any effective unitary ring  $R$  with canonical representations; thus of course the rôle of  $\mathbb{D}$  can be assumed on one side by each effectively given domain/field, on the other side by, say,  $\mathbb{D}(\overline{\mathbf{x}})$ ,  $\mathbb{Q}(\overline{\mathbf{x}})$ , ... . Actually, if we are interested in polynomial rings with coefficients in  $\mathbb{R}$  or in a ring of analytical functions, since a given finite basis has a finite number of coefficients  $c_i \in R$ , the requirement that the data are effectively given essentially means that we need to provide the algebraically dependencies among such  $c_i$  (compare Remark 3.1.).
3. Condition (1), restricting the choice of  $<$  to a term-ordering satisfying Equation (3), grants that, for each  $i, j$ ,  $X_i x_j \in \mathbf{T}\{\mathcal{I}\}$  and thus that  $C \subset G$ ; moreover, since there is no possible match among the leading terms  $\{X_i x_j : X_i \in \overline{\mathbf{v}}, x_j \in \overline{\mathbf{v}}\}$ , it also grants that, in  $Q$  and under  $<$ ,  $C$  is a bilateral Gröbner basis of the ideal  $\mathbb{I}_2(C)$  it generates.

Since there are the obvious matches

$$\{\mathbf{T}(f_{ij}) * \tau - X_i * x_j \tau : X_i \in \overline{\mathbf{V}}, x_j \tau \in \mathbf{T}\{G_0\}\}$$

in general we cannot expect that  $G_0 \cup C$  is a bilateral Gröbner basis of the ideal  $\mathbb{I}_2(G_0 \cup C)$  it generates; this in turn implies that as left  $R$ -module,  $\mathcal{Q}/\mathbb{I}_2(G_0 \cup C)$  is *not* necessarily free (see Example 7).

4. In the next sections we will discuss expressions

$$f = \sum_{l=1}^{\mu} a_l \lambda_l \star g_l \star b_l \rho_l : \lambda_l, \rho_l \in \mathcal{B}, a_l \in R_{\lambda_l} \setminus \{0\}, b_l \in R_{\rho_l} \setminus \{0\}, g_l \in B$$

where  $f \in M$  is an element and  $B \subset M$  is a basis of a bilateral  $\mathcal{A}$ -module  $M$ . Each element  $a_l \in R_{\lambda_l} \setminus \{0\}$  is to be considered either

- as any non-zero element in a residue class modulo the left ideal  $\mathcal{I}_{\lambda_l}$  in the ring  $\mathcal{R} = \mathbb{Z}\langle\overline{\mathbf{V}}\rangle$  or
- as the Zacharias canonical representation of such residue class in the set  $\mathbf{Zach}_{<}(R_{\lambda_l}) \subset \mathbf{Zach}_{<}(R) \subset \mathcal{R}$ , or even
- as any non-zero element in a residue class modulo the left ideal  $\pi(\mathcal{I}_{\lambda_l})$  in the ring  $R$  by simply identifying  $R$  with its Zacharias canonical representation  $\mathbf{Zach}_{<}(R)$ .

Consequently each element  $a_l \lambda_l$  represents a “monomial” in  $\mathcal{A}$  where the coefficient  $a_l$  can be interpreted either in  $R$  or in  $\mathcal{R}$  but in both cases represents a residue class or its canonical representation.

As a consequence, in all setting in which  $\mathcal{A}$  is mainly considered as a left  $R$ -module, we choose of writing  $a_l \in R \setminus \{0\}$ .

5. Each free  $\mathcal{A}$ -module  $\mathcal{A}^m, m \in \mathbb{N}$ , – the canonical basis of which will be denoted by  $\{\mathbf{e}_1, \dots, \mathbf{e}_m\}$  – is an  $R$ -module with basis the set of the *terms*

$$\mathcal{B}^{(m)} := \{t\mathbf{e}_i : t \in \mathcal{B}, 1 \leq i \leq m\}$$

and the projection  $\Pi : \mathcal{Q} := \mathbb{D}\langle\overline{\mathbf{Z}}\rangle \twoheadrightarrow \mathcal{A}, \mathcal{I} := \ker(\Pi), \mathcal{A} = \mathcal{Q}/\mathcal{I}$ , extends to each canonical projection, still denoted  $\Pi$ ,

$$\Pi : \mathcal{Q}^m \twoheadrightarrow \mathcal{A}^m, \ker(\Pi) = \mathcal{I}^m = \mathbb{I}_2(G^{(m)})$$

where  $G$  is the Gröbner basis w.r.t.  $<$  of  $\mathcal{I}$  and  $G^{(m)} := \{g\mathbf{e}_i, g \in G, 1 \leq i \leq m\}$  is the Gröbner basis of  $\mathcal{I}^m$  w.r.t. any term-ordering on  $\langle\overline{\mathbf{Z}}\rangle^{(m)}$  — which we still denote  $<$  with a slight abuse of notation — satisfying, for each  $t_1, t_2 \in \langle\overline{\mathbf{Z}}\rangle, \tau_1, \tau_2 \in \langle\overline{\mathbf{Z}}\rangle^{(m)}$ ,

$$t_1 \leq t_2, \tau_1 \leq \tau_2 \implies t_1 \tau_1 \leq t_2 \tau_2, \tau_1 t_1 \leq \tau_2 t_2.$$

□

In connection with the choice of the order module

$$\mathcal{B} = \mathbf{R}(\mathcal{I}) \sqcup \mathbf{N}(\mathcal{I}) = \langle \bar{\mathbf{V}} \rangle \setminus \mathbf{L}(\mathcal{I}) \subset \langle \bar{\mathbf{V}} \rangle$$

as module basis of  $\mathcal{A}$ , Spear's Theorem [26, IV.50.6.3] suggests to consider it well-ordered by the same term-ordering  $<$  on  $\langle \bar{\mathbf{Z}} \rangle$  which we have used for providing the Zacharias representation of  $\mathcal{A}$  discussed above and which in particular satisfies Equations (2) and (3). In fact, in our setting Spear states that, for any module  $\mathbf{M} \subset \mathcal{A}^m$ , denoting  $\mathbf{M}' := \Pi^{-1}(\mathbf{M}) = \mathbf{M} + \mathcal{I}^m$ , we have

1. if  $F$  is a reduced Gröbner basis of  $\mathbf{M}'$ , then

$$\{g \in F : g = \Pi(g)\} = \{\Pi(g) : g \in F, \mathbf{T}(g) \in \mathcal{B}^{(m)}\} = F \cap \mathbf{Zach}_{<}(\mathcal{A})^m$$

is a Gröbner basis of  $\mathbf{M}$ ;

2. if  $F \subset \mathbf{Zach}_{<}(\mathcal{A})^m$  – so that in particular  $\Pi(f) = f$  for each  $f \in F$  – is the Gröbner basis of  $\mathbf{M}$ , then  $F \sqcup G^{(m)}$  is a Gröbner basis of  $\mathbf{M}'$ .

Thus, w.r.t. a term-ordering  $<$  satisfying Equations (2) and (3), each non-zero element  $f \in \mathcal{A}^{(m)}$  has its canonical representation

$$f := \sum_{j=1}^s c(f, t_j \mathbf{e}_{\iota_j}) t_j \mathbf{e}_{\iota_j} \in \mathbf{Zach}_{<}(\mathcal{A})^m, t_j \in \mathcal{B}, c(f, t_j \mathbf{e}_{\iota_j}) \in R_{\iota_j} \setminus \{0\}, 1 \leq \iota_j \leq m,$$

with  $t_1 \mathbf{e}_{\iota_1} > t_2 \mathbf{e}_{\iota_2} > \dots > t_s \mathbf{e}_{\iota_s}$  and we denote,  $\text{supp}(f) := \{t_j \mathbf{e}_{\iota_j} : 1 \leq j \leq m\}$  the *support* of  $f$ ,  $\mathbf{T}_{<}(f) := t_1 \mathbf{e}_{\iota_1}$  its *maximal term*,  $\text{lc}_{<}(f) := c(f, t_1 \mathbf{e}_{\iota_1})$  its *leading coefficient* and  $\mathbf{M}_{<}(f) := c(f, t_1 \mathbf{e}_{\iota_1}) t_1 \mathbf{e}_{\iota_1}$  its *maximal monomial*.

If we denote, following [35, 36],  $\mathbf{M}(\mathcal{A}^m) := \{ct\mathbf{e}_i : t \in \mathcal{B}, c \in R_t \setminus \{0\}, 1 \leq i \leq m\}$ , the unique finite representation above can be reformulated

$$f = \sum_{\tau \in \text{supp}(f)} m_{\tau}, m_{\tau} = c(f, \tau) \tau$$

as a sum of elements of the *monomial set*  $\mathbf{M}(\mathcal{A}^m)$ .

These notions heavily depend on Zacharias representation which in turn depends on the term-ordering  $<$  we have fixed on  $\langle \bar{\mathbf{V}} \rangle$ .

This has an unexpected advantage: already in the case of *semigroup rings* [37, 20, 21]  $\mathcal{A} = R[\mathbf{S}]$ , an elementary adaptation of Buchberger Theory (which would suggest to set  $\mathcal{B} := \mathbf{S}$ ) is impossible since  $\mathbf{S}$  does not possess a semigroup ordering. The paradoxical solution consists [20, 21], or at least can be interpreted as [26, IV.50.13.5] considering  $\mathbf{S} := \mathcal{B}$  not as a semigroup but as a subset of a proper free semigroup  $\langle \bar{\mathbf{V}} \rangle \supset \mathcal{B}$  and, via Spear's Theorem, import to  $\mathcal{A}$  the *natural*  $\langle \bar{\mathbf{V}} \rangle$ -*pseudoevaluation*

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \mapsto \mathbf{T}(f)$$

of  $R\langle \bar{\mathbf{V}} \rangle$ .

The general solution, thus, consists into applying the classical filtration/valuation interpretation of Buchberger Theory [41, 24, 1, 29] and to impose on  $\mathcal{Q}$  a  $\Gamma$ -pseudovaluation

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} \subset \Gamma^{(m)} : f \rightarrow \mathbf{T}(f)$$

where the semigroup  $(\Gamma, \circ)$ ,  $\mathcal{B} \subset \Gamma \subset \langle \bar{\mathbf{V}} \rangle$ , is properly chosen on the basis of the structural properties of the relation ideal  $\mathcal{I}$  in order to obtain a smoother arithmetics of the associated graded ring  $\mathcal{G} := G(\mathcal{A})$ .

## 4 Apel: pseudovaluation

Denote, for a semigroup  $(\Gamma, \circ)$ ,  $\Gamma^{(u)}$  the sets

$$\Gamma^{(u)} := \{\gamma e_i, \gamma \in \Gamma, 1 \leq i \leq u\}, u \in \mathbb{N},$$

endowed with no operation except the natural action of  $\Gamma$

$$\Gamma \times \Gamma^{(u)} \times \Gamma \rightarrow \Gamma^{(u)} : (\delta_l, \gamma, \delta_r) \mapsto \delta_l \circ \gamma \circ \delta_r, \text{ for each } \delta_l, \delta_r \in \Gamma, \gamma \in \Gamma^{(u)}.$$

**Definition 9.** If  $(\Gamma, \circ)$  is a semigroup, a ring  $\mathcal{A}$  is called a  $\Gamma$ -graded ring if there is a family of subgroups  $\{\mathcal{A}_\gamma : \gamma \in \Gamma\}$  such that

- $\mathcal{A} = \bigoplus_{\gamma \in \Gamma} \mathcal{A}_\gamma$ ,
- $\mathcal{A}_\delta \mathcal{A}_\gamma \subset \mathcal{A}_{\delta \circ \gamma}$  for any  $\delta, \gamma \in \Gamma$ .

A right  $\mathcal{A}$ -module  $M$  of a  $\Gamma$ -graded ring  $\mathcal{A}$  is called a  $\Gamma^{(u)}$ -graded  $\mathcal{A}$ -module if there is a family of subgroups  $\{M_\gamma : \gamma \in \Gamma^{(u)}\}$  such that

- $M = \bigoplus_{\gamma \in \Gamma^{(u)}} M_\gamma$ ,
- $M_\gamma \mathcal{A}_\delta \subset M_{\gamma \circ \delta}$  for any  $\delta \in \Gamma, \gamma \in \Gamma^{(u)}$ .

Given two  $\Gamma^{(u)}$ -graded right  $\mathcal{A}$ -modules  $M, N$ , by a  $\Gamma$ -graded morphism  $\phi : M \rightarrow N$  of degree  $\delta \in \Gamma$  we shall mean a morphism such that  $\phi(M_\gamma) \subset N_{\gamma \circ \delta}$  for each  $\gamma \in \Gamma^{(u)}$ .

An  $\mathcal{A}$ -bimodule  $M$  of a  $\Gamma$ -graded ring  $\mathcal{A}$  is called a  $\Gamma^{(u)}$ -graded  $\mathcal{A}$ -bimodule if there is a family of subgroups  $\{M_\gamma : \gamma \in \Gamma^{(u)}\}$  such that

- $M = \bigoplus_{\gamma \in \Gamma^{(u)}} M_\gamma$ ,
- $\mathcal{A}_\delta M_\gamma \subset M_{\delta \circ \gamma}$  and  $M_\gamma \mathcal{A}_\delta \subset M_{\gamma \circ \delta}$  for any  $\delta \in \Gamma, \gamma \in \Gamma^{(u)}$ .

Given two  $\Gamma^{(u)}$ -graded  $\mathcal{A}$ -bimodules  $M, N$  by a  $\Gamma$ -graded morphism  $\phi : M \rightarrow N$  of degree  $(\delta_l, \delta_r) \in \Gamma^2$ , we shall mean a morphism such that  $\phi(M_\gamma) \subset N_{\delta_l \circ \gamma \circ \delta_r}$  for each  $\gamma \in \Gamma^{(u)}$ .

Each element  $x \in M_\gamma$  is called *homogeneous* of degree  $\gamma \in \Gamma^{(u)}$ .

Each element  $x \in M$  can be uniquely represented as a finite sum  $x := \sum_{\gamma \in \Gamma^{(u)}} x_\gamma$  where  $x_\gamma \in M_\gamma$  and  $\{\gamma : x_\gamma \neq 0\}$  is finite; each such element  $x_\gamma$  is called a *homogeneous component* of degree  $\gamma$ .  $\square$

**Definition 10** (Apel). [1] Let  $(\Gamma, \circ)$  be a semigroup well-ordered by a semigroup ordering  $<$ ,  $\mathcal{A}$  a ring which is a left  $R$ -module over a subring  $R \subset \mathcal{A}$  and  $M$  an  $\mathcal{A}$ -module.

A  $\Gamma$ -pseudoevaluation is a function  $v : \mathcal{A} \setminus \{0\} \mapsto \Gamma$  such that, for each  $a_1, a_2 \in \mathcal{A} \setminus \{0\}$ ,

1.  $v(a_1 - a_2) \leq \max(v(a_1), v(a_2))$ ,
2.  $v(a_1 a_2) \leq v(a_1) \circ v(a_2)$ ,
3.  $v(r) = \mathbf{1}_\Gamma$  for each  $r \in R \subset \mathcal{A}$ .

Impose now on  $\Gamma^{(u)}$  a well-ordering, denoted, with a slight abuse of notation also  $<$ , satisfying, for each  $\delta_1, \delta_2 \in \Gamma, \gamma_1, \gamma_2 \in \Gamma^{(u)}$

$$\delta_1 \leq \delta_2, \gamma_1 \leq \gamma_2 \implies \delta_1 \circ \gamma_1 \leq \delta_2 \circ \gamma_2, \gamma_1 \circ \delta_1 \leq \gamma_2 \circ \delta_2.$$

A function  $w : M \setminus \{0\} \mapsto \Gamma^{(u)}$  is said a  $v$ -compatible  $\Gamma^{(u)}$ -pseudoevaluation on  $M$  if it satisfies, for each  $a \in \mathcal{A} \setminus \{0\}$  and each  $m, m_1, m_2 \in M \setminus \{0\}$ ,

4.  $w(m_1 - m_2) \leq \max(w(m_1), w(m_2))$ ,
5.  $w(am) \leq v(a) \circ w(m)$  and  $w(ma) \leq w(m) \circ v(a)$ .

□

*Notation 11.* (Cf. [26, II.Definition 24.6.5]) Given a semigroup  $(\Gamma, \circ)$  well-ordered by a semigroup ordering  $<$ , a ring  $\mathcal{A}$  which is a left  $R$ -module over a subring  $R \subset \mathcal{A}$ , a  $\Gamma$ -pseudoevaluation  $v : \mathcal{A} \setminus \{0\} \mapsto \Gamma$ , an  $\mathcal{A}$ -bimodule  $M$  and a  $v$ -compatible  $\Gamma^{(u)}$ -pseudoevaluation  $w : M \setminus \{0\} \mapsto \Gamma^{(u)}$  write

- $F_\gamma(M) := \{m \in M : w(m) \leq \gamma\} \cup \{0\} \subset M$ , for each  $\gamma \in \Gamma^{(u)}$ ;
- $V_\gamma(M) := \{m \in M : w(m) < \gamma\} \cup \{0\} \subset M$ , for each  $\gamma \in \Gamma^{(u)}$ ;
- $G_\gamma(M) := F_\gamma(M)/V_\gamma(M)$ , for each  $\gamma \in \Gamma^{(u)}$ ;
- $G(M) := \bigoplus_{\gamma \in \Gamma^{(u)}} G_\gamma(M)$ .
- $\mathcal{L} : M \mapsto G(M)$  is the map such that, for each  $m \in M, m \neq 0$ ,  $\mathcal{L}(m)$  denotes the residue class of  $m \bmod V_{w(m)}(M)$  and  $\mathcal{L}(0) = 0$ . □

**Definition 12.** With the present notation, we define

- the *associated graded ring* of  $\mathcal{A}$  the left  $R$ -module  $G(\mathcal{A})$  which is a  $\Gamma$ -graded ring, and
- the *associated graded module* of  $M$  the left  $R$ -module  $G(M)$ , which is a  $\Gamma^{(u)}$ -graded  $G(\mathcal{A})$ -module. □

As we have remarked above, when the ring  $\mathcal{A}$  is explicitly given via the Zacharias representation (5) we cannot use the function

$$\mathbf{T}(\cdot) : \mathcal{A} \mapsto \mathcal{B} : f \mapsto \mathbf{T}(f)$$

as a natural pseudovaluation because, in general, either  $\mathcal{B}$  is not a semigroup or, at least,  $<$  is not a semigroup ordering on it.

Thus we consider a semigroup  $\Gamma$ ,  $\mathcal{B} \subset \Gamma \subset \langle \bar{\mathbf{V}} \rangle$ , such that the restriction of  $<$  on  $\Gamma$  is a semigroup ordering. In this way, the function

$$\mathbf{T}(\cdot) : \mathcal{A} \mapsto \mathcal{B} \subset \Gamma : f \rightarrow \mathbf{T}(f)$$

is a  $\Gamma$ -pseudovaluation, which we will call its *natural  $\Gamma$ -pseudovaluation* and the free  $\mathcal{A}$ -module  $\mathcal{A}^m$  has the *natural  $\mathbf{T}(\cdot)$ -compatible pseudovaluation*

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} \subset \Gamma^{(m)} : f \rightarrow \mathbf{T}(f).$$

Under these natural pseudovaluations, we have

- $G_\delta(\mathcal{A}) \cong R_\delta$  for each  $\delta \in \mathcal{B}$  and
- $G_\delta(\mathcal{A}) = \{0\}$  for each  $\delta \in \Gamma \setminus \mathcal{B}$ ;
- $G(\mathcal{A})$  and  $\mathcal{A}$  coincide as subsets, (but not as rings nor as  $R$ -modules) and both have the Zacharias representation stated in (5);
- $G_\gamma(\mathcal{A}^m) \cong R_\delta$  for each  $\gamma = \delta \mathbf{e}_i \in \mathcal{B}^{(m)}$  and
- $G_\gamma(\mathcal{A}^m) = \{0\}$  for each  $\gamma \in \Gamma^{(m)} \setminus \mathcal{B}^{(m)}$ ;
- $G(\mathcal{A}^m) = G(\mathcal{A})^m$  as  $R$ -modules.
- $\mathcal{L}(f) = \mathbf{M}(f)$  for each  $f \in \mathcal{A}^m$ .

## 5 Bilateral Gröbner bases

Let  $\mathcal{A} = Q/I$  be an effectively given left  $R$ -module, endowed with its natural  $\Gamma$ -pseudovaluation  $\mathbf{T}(\cdot)$  where the semigroup  $(\Gamma, \circ)$  satisfies

- $\mathcal{B} \subset \Gamma \subset \langle \bar{\mathbf{V}} \rangle$  and
- the restriction of  $<$  on  $\Gamma$  is a semigroup ordering.

We denote  $\mathcal{G} = G(\mathcal{A})$ , by  $\star$  the multiplication of  $\mathcal{A}$  and by  $*$  the one of  $\mathcal{G}$ .

For any set  $F \subset \mathcal{A}^m$  we denote, in function of  $<$ :

- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\} \subset \mathcal{B}^{(m)}$ ;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\} \subset \mathbf{M}(\mathcal{A}^m)$ .
- $\mathbf{T}_2(F) := \mathbb{I}_2(\mathbf{T}\{F\}) = \{\mathbf{T}(\lambda \star f \star \rho) : \lambda, \rho \in \mathcal{B}, f \in F\} = \{\lambda \circ \mathbf{T}(f) \circ \rho : \lambda, \rho \in \mathcal{B}, f \in F\} \subset \mathcal{B}^{(m)}$ ;
- $\mathbf{M}_2(F) := \{\mathbf{M}(a\lambda \star f \star b\rho) : a \in R_\lambda \setminus \{0\}, b \in R_\rho \setminus \{0\}, \lambda, \rho \in \mathcal{B}, f \in F\} = \{m * \mathbf{M}(f) * n : m, n \in \mathbf{M}(\mathcal{A}), f \in F\} \subset \mathbf{M}(\mathcal{A}^m)$ .



**Definition 13.** Let  $M \subset \mathcal{A}^m$  be a bilateral  $\mathcal{A}$ -module.  $F \subset M$  will be called

- a bilateral *Gröbner basis* of  $M$  if  $F$  satisfies

$$\mathbf{M}\{M\} = \mathbf{M}_2(M) = \mathbf{M}\{\mathbb{I}_2(\mathbf{M}_2(F))\} = \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\} = \mathbb{I}_2(\mathbf{M}\{F\}) \cap \mathbf{M}(\mathcal{A}^m),$$

id est if it satisfies the following condition:

- for each  $f \in M$ , there are  $g_i \in F$ ,  $\lambda_i, \rho_i \in \mathcal{B}$ ,  $a_i \in R_{\lambda_i} \setminus \{0\}$ ,  $b_i \in R_{\rho_i} \setminus \{0\}$  such that
  - $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$  for all  $i$ ,
  - $\mathbf{M}(f) = \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i$ ;
- a bilateral *strong Gröbner basis* of  $M$  if it satisfies the following equivalent conditions:
  - for each  $f \in M$  there is  $g \in F$  such that  $\mathbf{M}(g) \mid_2 \mathbf{M}(f)$ ,
  - for each  $f \in M$  there are  $g \in F$ ,  $a \in R_\lambda \setminus \{0\}$ ,  $b \in R_\rho \setminus \{0\}$ ,  $\lambda, \rho \in \mathcal{B}$  such that  $\mathbf{M}(f) = a\lambda * \mathbf{M}(g) * b\rho = \mathbf{M}(a\lambda \star g \star b\rho)$ ,
  - $\mathbf{M}\{M\} = \mathbf{M}_2(M) = \mathbf{M}_2(F)$ .

**Definition 14.** Let  $M \subset \mathcal{A}^m$  be a bilateral  $\mathcal{A}$ -module and  $F \subset M$ . We say that  $f \in \mathcal{A}^m \setminus \{0\}$  has

- a bilateral (weak) *Gröbner representation* in terms of  $F$  if it can be written as  $f = \sum_{i=1}^\mu a_i \lambda_i \star g_i \star b_i \rho_i$ , with  $\lambda_i, \rho_i \in \mathcal{B}$ ,  $a_i \in R_{\lambda_i} \setminus \{0\}$ ,  $b_i \in R_{\rho_i} \setminus \{0\}$ ,  $g_i \in F$ , and  $\mathbf{T}(f) \geq \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$  for each  $i$ ;
- a bilateral *strong Gröbner representation* in terms of  $F$  if it can be written as  $f = \sum_{i=1}^\mu a_i \lambda_i \star g_i \star b_i \rho_i$ , with  $\lambda_i, \rho_i \in \mathcal{B}$ ,  $a_i \in R_{\lambda_i} \setminus \{0\}$ ,  $b_i \in R_{\rho_i} \setminus \{0\}$ ,  $g_i \in F$ , and  $\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(g_1) \circ \rho_1 > \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$  for each  $i$ ,  $1 < i \leq \mu$ .

For  $f \in \mathcal{A}^m \setminus \{0\}$ ,  $F \subset \mathcal{A}^m$ , an element  $g := \text{NF}(f, F) \in \mathcal{A}^m$  is called a

- bilateral (weak) *normal form* of  $f$  w.r.t.  $F$ , if

$$\begin{aligned} f - g &\in \mathbb{I}_2(F) \text{ has a weak Gröbner representation wrt } F \text{ and} \\ g \neq 0 &\implies \mathbf{M}(g) \notin \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\}; \end{aligned}$$

- bilateral *strong normal form* of  $f$  w.r.t.  $F$ , if

$$\begin{aligned} f - g &\in \mathbb{I}_2(F) \text{ has a strong Gröbner representation wrt } F \text{ and} \\ g \neq 0 &\implies \mathbf{M}(g) \notin \mathbf{M}_2(F). \end{aligned}$$

*Remark 15.* As we noted above,  $\mathcal{G} := G(\mathcal{A})$  and  $\mathcal{A}$ , while coinciding as sets, do not necessarily coincide as rings nor as  $R$ -modules; thus in general for  $\lambda, \rho \in \mathcal{B}$ ,  $a \in R_\lambda \setminus \{0\}$ ,  $b \in R_\rho \setminus \{0\}$  and  $g \in \mathcal{A}^m$ ,  $g = \mathbf{M}(g) + p$ , we don't have  $a\lambda \star \mathbf{M}(g) \star b\rho = a\lambda * \mathbf{M}(g) * b\rho$  but we could have

$$\text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho) := a\lambda \star \mathbf{M}(g) \star b\rho - a\lambda * \mathbf{M}(g) * b\rho \neq 0.$$

In such case, of course,  $\mathbf{T}(\text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho)) < \mathbf{T}(a\lambda \star \mathbf{M}(g) \star b\rho)$ ; more exactly, either

–  $\lambda \circ \mathbf{T}(g) \circ \rho \in \mathcal{B}^{(m)}$  in which case

$$\mathbf{M}(a\lambda \star \mathbf{M}(g) \star b\rho) = a\lambda * \mathbf{M}(g) * b\rho$$

$$\text{and } a\lambda \star \mathbf{M}(g) \star b\rho = \mathbf{M}(a\lambda \star \mathbf{M}(g) \star b\rho) + \text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho);$$

– or  $\lambda \circ \mathbf{T}(g) \circ \rho \in \Gamma^{(m)} \setminus \mathcal{B}^{(m)}$  in which case

$$a\lambda * \mathbf{M}(g) * b\rho = \mathbf{M}(a\lambda \star \mathbf{M}(g) \star b\rho) = 0 \text{ and } a\lambda \star \mathbf{M}(g) \star b\rho = \text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho);$$

in both cases we have

$$\begin{aligned} a\lambda \star g \star b\rho - a\lambda * \mathbf{M}(g) * b\rho &= a\lambda \star \mathbf{M}(g) \star b\rho - a\lambda * \mathbf{M}(g) * b\rho + a\lambda \star p \star b\rho \\ &= \text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho) + a\lambda \star p \star b\rho =: h, \end{aligned}$$

with  $\mathbf{T}(h) < \lambda \circ \mathbf{T}(g) \circ \rho$ .  $\square$

**Lemma 16.** *Let  $f \in \mathcal{A}^m$ ; then for each  $g_i \in \mathcal{A}^m$ ,  $\lambda_i, \rho_i \in \mathcal{B}$ ,  $a_i \in R_{\lambda_i} \setminus \{0\}$ ,  $b_i \in R_{\rho_i} \setminus \{0\}$  which satisfy*

–  $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$ , for each  $i$ ,

*the following are equivalent*

1.  $\mathbf{M}(f) = \sum_i \mathbf{M}(a_i \lambda_i \star g_i \star b_i \rho_i)$ ,
2.  $\mathbf{M}(f) = \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i$ ,
3.  $\mathbf{T}(f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i) < \mathbf{T}(f)$ .

*Proof.* Remark that the assumption  $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$ , for each  $i$ , grants, according Remark 15, the equivalence (1)  $\iff$  (2).

Moreover, denoting  $q := f - \mathbf{M}(f)$ ,  $p_i := g_i - \mathbf{M}(g_i)$ ,

$$h_i := a_i \lambda_i \star g_i \star b_i \rho_i - a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i = \text{tail}(a_i \lambda_i \star \mathbf{M}(g_i) \star b_i \rho_i) + a_i \lambda_i \star p_i \star b_i \rho_i$$

and  $h := q - \sum_i h_i$  we have

$$\begin{aligned} f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i &= \mathbf{M}(f) + q - \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i - \sum_i h_i \\ &= \mathbf{M}(f) - \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i + h. \end{aligned}$$

Thus, setting  $\tau := \mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i \in \mathcal{B}^{(m)}$ , we have  $\mathbf{T}(q) < \tau$  and  $\mathbf{T}(h_i) < \tau$  for each  $i$ , so that  $\mathbf{T}(h) < \tau$ .

Therefore  $\mathbf{M}(f) = \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i = \sum_i \mathbf{M}(a_i \lambda_i \star g_i \star b_i \rho_i)$  implies

$$f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i = h$$

so that  $\mathbf{T}(f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i) = \mathbf{T}(h) < \mathbf{T}(f)$  proving (2)  $\implies$  (3).

Conversely,

$$\mathbf{T}\left(f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i\right) < \mathbf{T}(f) \implies \mathbf{M}(f) - \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i = 0.$$

□

**Theorem 17.** For any set  $F \subset \mathcal{A}^m \setminus \{0\}$ , among the following conditions:

1.  $f \in \mathbb{I}_2(F) \iff$  it has a bilateral strong Gröbner representation

$$f = \sum_{i=1}^{\mu} a_i \lambda_i \star g_i \star b_i \rho_i$$

in terms of  $F$  which further satisfies

$$\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(g_1) \circ \rho_1 \text{ and } \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i > \lambda_{i+1} \circ \mathbf{T}(g_{i+1}) \circ \rho_{i+1} \text{ for each } i;$$

2.  $f \in \mathbb{I}_2(F) \iff$  it has a bilateral strong Gröbner representation in terms of  $F$ ;
3.  $F$  is a bilateral strong Gröbner basis of  $\mathbb{I}_2(F)$ ;
4. for each  $f \in \mathcal{A}^m \setminus \{0\}$  and any bilateral strong normal form  $h$  of  $f$  w.r.t.  $F$  we have  $f \in \mathbb{I}_2(F) \iff h = 0$ ;
5.  $f \in \mathbb{I}_2(F) \iff$  it has a bilateral weak Gröbner representation in terms of  $F$ ;
6.  $F$  is a bilateral weak Gröbner basis of  $\mathbb{I}_2(F)$ ;
7. for each  $f \in \mathcal{A}^m \setminus \{0\}$  and any bilateral weak normal form  $h$  of  $f$  w.r.t.  $F$  we have  $f \in \mathbb{I}_2(F) \iff h = 0$ ;

there are the implications

$$\begin{array}{ccccccc} (1) & \iff & (2) & \iff & (3) & \iff & (4) \\ & & \Downarrow & & \Downarrow & & \Downarrow \\ & & (5) & \iff & (6) & \iff & (7) \end{array}$$

If  $R$  is a skew field we have also the implication  $(5) \implies (2)$  and as a consequence the seven conditions are equivalent.

*Proof.* The implications  $(1) \implies (2) \implies (3)$ ,  $(5) \implies (6)$ ,  $(2) \implies (5)$ ,  $(3) \implies (6)$  and  $(4) \implies (7)$  are trivial.

Ad  $(3) \implies (1)$ : for each  $f \in \mathbb{I}_2(F)$  by assumption there are elements  $g \in F$ ,  $\lambda, \rho \in \mathcal{B}$ ,  $a \in R_\lambda \setminus \{0\}$ ,  $b \in R_\rho \setminus \{0\}$ , such that

$$\mathbf{T}(f) = \lambda \circ \mathbf{T}(g) \circ \rho \text{ and } \mathbf{M}(f) = a\lambda * \mathbf{M}(g) * b\rho.$$

Thus  $\mathbf{M}(a\lambda \star \mathbf{M}(g) \star b\rho) = a\lambda * \mathbf{M}(g) * b\rho = \mathbf{M}(f)$  and denoting, for  $f = \mathbf{M}(f) + q$  and  $g = \mathbf{M}(g) + p$ ,

$$f_1 := f - a\lambda \star g \star b\rho = q - \text{tail}(a\lambda \star \mathbf{M}(g) \star b\rho) - a\lambda \star p \star b\rho$$

we have  $\mathbf{T}(f_1) < \mathbf{T}(f)$  so the claim follows by induction, since  $\mathcal{B}^{(m)}$  is well-ordered by  $<$ .

Ad (6)  $\implies$  (5): similarly, for each  $f \in \mathbb{I}_2(F)$  by assumption there are elements  $g_i \in F$ ,  $\lambda_i, \rho_i \in \mathcal{B}$ ,  $a_i \in R_{\lambda_i} \setminus \{0\}$ ,  $b_i \in R_{\rho_i} \setminus \{0\}$  such that

- $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$  for all  $i$ ,
- $\mathbf{M}(f) = \sum_i a_i \lambda_i * \mathbf{M}(g_i) * b_i \rho_i$ .

Thus  $\mathbf{T}(f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i) < \mathbf{T}(f)$  and it is then sufficient to denote  $f_1 := f - \sum_i a_i \lambda_i \star g_i \star b_i \rho_i$  in order to deduce the claim by induction.

Ad (3)  $\implies$  (4) and (6)  $\implies$  (7): either

- $h = 0$  and  $f = f - h \in \mathbb{I}_2(F)$  or
- $h \neq 0$ ,  $\mathbf{M}(h) \notin \mathbf{M}(\mathbb{I}_2(F))$ ,  $h \notin \mathbb{I}_2(F)$  and  $f \notin \mathbb{I}_2(F)$ .

Ad (4)  $\implies$  (2) and (7)  $\implies$  (5): for each  $f \in \mathbb{I}_2(F)$ , its normal form is  $h = 0$  and  $f = f - h$  has a strong (resp.: weak) Gröbner representation in terms of  $F$ .

Ad (5)  $\implies$  (2): let  $f \in \mathbb{I}_2(F) \setminus \{0\}$ ; since  $R$  is a skew field, (5) implies the existence of elements  $g \in F$ ,  $\lambda, \rho \in \mathcal{B}$ , such that  $\mathbf{T}(f) = \lambda \circ \mathbf{T}(g) \circ \rho =: \tau$ ; thus denoting  $d \in R \setminus \{0\}$  the value which satisfies

$$d\tau = \mathbf{M}(\lambda \star g \star \rho) = \lambda * \mathbf{M}(g) * \rho,$$

we have

$$\mathbf{M}(f) = \text{lc}(f)d^{-1}d\tau = \text{lc}(f)d^{-1}\lambda * \mathbf{M}(g) * \rho = \mathbf{M}((\text{lc}(f)d^{-1}\lambda) \star g \star \rho)$$

as required.  $\square$

## 6 Weispfenning multiplication

In proposing a Buchberger Theory for a class of Ore-like rings, *id est* Weispfenning rings [44], [26, IV.49.11, IV.50.13.6]  $\mathbb{Q}\langle x, Y \rangle / \mathbb{I}(Yx - x^e Y)$ ,  $e \in \mathbb{N}$ ,  $e > 1$ , Weispfenning considered, given a basis  $F$ , the restricted module

$$\mathbb{I}_W(F) := \text{Span}_{\mathbb{Q}}\{x^a f Y^b, (a, b) \in \mathbb{N}^2\}$$

and computed a restricted Gröbner bases  $G$  which grants to each element  $f \in \mathbb{I}_W(F)$  a restricted Gröbner representation

$$f = \sum_{i=1}^{\mu} c_i x^{a_i} g_i Y^{b_i} : \deg_Y(f) \geq \deg_Y(g_i) + b_i, c_i \in \mathbb{Q}, (a_i, b_i) \in \mathbb{N}^2, g_i \in G,$$

to be extended, in a second step, to the required basis by an adaptation of Kandri-Rody—Weispfenning completion [15][26, IV.49.5.2].

We can interpret this construction as a multiplication on the monomial set

$$\mathbf{M}(\mathcal{A}) := \{ct : t \in \mathcal{B}, c \in R_t \setminus \{0\}\}$$

which becomes, by distribution, a multiplication in  $\mathcal{A}$ .

**Definition 18.** Setting, for each  $m_1 = a_1\tau_1, m_2 = a_2\tau_2 \in M(\mathcal{A})$

$$m_1 \diamond m_2 := (a_1 a_2)(\tau_2 \circ \tau_1)$$

Weispfenning multiplication is the associative multiplication

$$\diamond : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$$

defined as

$$f \diamond g = \sum_{\tau \in \text{supp}(f)} \sum_{\omega \in \text{supp}(g)} m_\tau \diamond n_\omega = \sum_{\tau \in \text{supp}(f)} \sum_{\omega \in \text{supp}(g)} c(f, \tau) c(g, \omega) \omega \tau$$

for each  $f = \sum_{\tau \in \text{supp}(f)} m_\tau, m_\tau = c(f, \tau)\tau$  and  $g = \sum_{\omega \in \text{supp}(g)} n_\omega, n_\omega = c(g, \omega)\omega$ .

Note that  $\diamond$  is commutative when  $\mathcal{A}$  is a twisted monoid ring  $R[\mathbf{S}]$  over a commutative ring  $R$  and a commutative monoid  $\mathbf{S}$ , as polynomial rings, solvable polynomial rings [15, 16], [26, IV.49.5], multivariate Ore extensions [30, 31, 8, 9] ...

The intuition of Weispfenning can be formulated by remarking that its effect is to transform a bilateral problem into a left one. Thus the construction proposed in [44] simply reformulates the one stated in [15]; in an analogous way the reformulation of the (commutative) Gebauer–Möller criteria [11] for detecting useless S-pairs was easily performed in [9] in the context of multivariate Ore extensions by means of Weispfenning multiplication.

Our aim is therefore to apply  $\diamond$  to reduce the computation of Gebauer–Möller sets for the bilateral case to the trivial right case where efficient solutions are already available [22], [26, IV.47.2.3].

We note that Weispfenning construction is a smoother special case of the construction proposed by Pritchard [33, 34], [26, IV.47.5] for reformulating bilateral modules in  $\mathbb{D}[\langle \bar{\mathbf{X}} \rangle]$  as left modules in a monoid ring  $\mathbb{D}[\langle \bar{\mathbf{X}} \rangle^*]$  where the monoid  $\langle \bar{\mathbf{X}} \rangle^*$  is properly defined in terms of  $\langle \bar{\mathbf{X}} \rangle$ .

## 7 Restricted Gröbner bases

Following Weispfenning’s intuition [44] we further denote

- $\mathbb{I}_W(F) \subset \mathcal{A}^m$  the *restricted* module generated by  $F$ ,

$$\begin{aligned} \mathbb{I}_W(F) &:= \text{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F), \\ &= \text{Span}_R(m \diamond f : m \in M(\mathcal{A}^m), f \in F), \end{aligned}$$

- $\mathbf{T}_W(F) := \mathbb{I}_R(\mathbf{T}\{F\}) = \{\mathbf{T}(f \star \rho) : \rho \in \mathcal{B}, f \in F\} = \{\mathbf{T}(f) \circ \rho : \rho \in \mathcal{B}, f \in F\} \subset \mathcal{B}^{(m)}$ ;
- $\mathbf{M}_W(F) := \{\mathbf{M}(af \star \rho) : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F\} = \{a\mathbf{M}(f) * \rho : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F\} = \{m \diamond \mathbf{M}(f) : m \in M(\mathcal{A}^m), f \in F\} \subset M(\mathcal{A}^m)$ .

**Definition 19.** Let  $M \subset \mathcal{A}^m$  be a restricted  $\mathcal{A}$ -module.  $F \subset M$  will be called

- a restricted *Gröbner basis* of  $\mathbf{M}$  if  $F$  satisfies

$$\mathbf{M}\{\mathbf{M}\} = \mathbf{M}_W(\mathbf{M}) = \mathbf{M}\{\mathbb{I}_W(\mathbf{M}_W(F))\} = \mathbf{M}\{\mathbb{I}_W(\mathbf{M}\{F\})\} = \mathbb{I}_W(\mathbf{M}\{F\}) \cap \mathbf{M}(\mathcal{A}^m),$$

if it satisfies the following condition:

- for each  $f \in \mathbf{M}$ , there are  $g_i \in F, \rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}$  such that
  - $\mathbf{T}(f) = \mathbf{T}(g_i) \circ \rho_i$  for all  $i$ ,
  - $\mathbf{M}(f) = \sum_i a_i \mathbf{M}(g_i) * \rho_i = \sum_i a_i \rho_i \diamond \mathbf{M}(g_i)$ ;
- a restricted *strong Gröbner basis* of  $\mathbf{M}$  if it satisfies the following equivalent conditions:

- for each  $f \in \mathbf{M}$  there is  $g \in F$  such that  $\mathbf{M}(g) \mid_W \mathbf{M}(f)$ ,
- for each  $f \in \mathbf{M}$  there are  $g \in F, a \in R \setminus \{0\}, \rho \in \mathcal{B}$  such that

$$\mathbf{M}(f) = a\mathbf{M}(g) * \rho = \mathbf{M}(ag \star \rho) = \mathbf{M}(a\rho \diamond g),$$

- $\mathbf{M}\{\mathbf{M}\} = \mathbf{M}_W(\mathbf{M}) = \mathbf{M}_W(F)$ .

**Definition 20.** Let  $\mathbf{M} \subset \mathcal{A}^m$  be a restricted  $\mathcal{A}$ -module and  $F \subset \mathbf{M}$ . We say that  $f \in \mathcal{A}^m \setminus \{0\}$  has

- a restricted (weak) *Gröbner representation* in terms of  $F$  if it can be written as  $f = \sum_{i=1}^{\mu} a_i g_i \star \rho_i = \sum_{i=1}^{\mu} a_i \rho_i \diamond g_i$ , with  $\rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}, g_i \in F$ , and  $\mathbf{T}(f) \geq \mathbf{T}(g_i) \circ \rho_i$  for each  $i$ ;
- a restricted *strong Gröbner representation* in terms of  $F$  if it can be written as  $f = \sum_{i=1}^{\mu} a_i g_i \star \rho_i = \sum_{i=1}^{\mu} a_i \rho_i \diamond g_i$ , with  $\rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}, g_i \in F$ , and  $\mathbf{T}(f) = \mathbf{T}(g_1) \circ \rho_1 > \mathbf{T}(g_i) \circ \rho_i$  for each  $i, 1 < i \leq \mu$ .

For  $f \in \mathcal{A}^m \setminus \{0\}, F \subset \mathcal{A}^m$ , an element  $g := \text{NF}(f, F) \in \mathcal{A}^m$  is called a

- restricted (weak) *normal form* of  $f$  w.r.t.  $F$ , if
  - $f - g \in \mathbb{I}_W(F)$  has a restricted weak Gröbner representation wrt  $F$ , and
  - $g \neq 0 \implies \mathbf{M}(g) \notin \mathbf{M}\{\mathbb{I}_W(\mathbf{M}\{F\})\}$ ;
- restricted *strong normal form* of  $f$  w.r.t.  $F$ , if
  - $f - g \in \mathbb{I}_W(F)$  has a restricted strong Gröbner representation wrt  $F$ , and
  - $g \neq 0 \implies \mathbf{M}(g) \notin \mathbf{M}_W(F)$ .

**Lemma 21.** Let  $f \in \mathcal{A}^m$ ; then for each  $g_i \in \mathcal{A}^m, \rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}$  which satisfy

- $\mathbf{T}(f) = \mathbf{T}(g_i) \circ \rho_i$ , for each  $i$ ,

the following are equivalent

1.  $\mathbf{M}(f) = \sum_i \mathbf{M}(a_i \rho_i \diamond g_i)$ ,

2.  $\mathbf{M}(f) = \sum_i a_i \mathbf{M}(g_i) * \rho_i$ ,
3.  $\mathbf{T}(f - \sum_i a_i \rho_i \diamond g_i) < \mathbf{T}(f)$ .

*Proof.* Remark that the assumption  $\mathbf{T}(f) = \mathbf{T}(g_i) \circ \rho_i$ , for each  $i$ , grants, according Remark 15, the equivalence (1)  $\iff$  (2).

Moreover, denoting, for each  $\rho \in \mathcal{B}$ ,  $a \in R \setminus \{0\}$  and  $g \in \mathcal{A}^m$

$$\text{tail}(a\rho \diamond \mathbf{M}(g)) := a\rho \diamond \mathbf{M}(g) - a\mathbf{M}(g) * \rho$$

and setting  $q := f - \mathbf{M}(f)$ ,  $p_i := g_i - \mathbf{M}(g_i)$ ,

$$h_i := a_i \rho_i \diamond g_i - a_i \mathbf{M}(g_i) * \rho_i = \text{tail}(a_i \rho_i \diamond \mathbf{M}(g_i)) + a_i \rho_i \diamond p_i$$

and  $h := q - \sum_i h_i$  we have

$$\begin{aligned} f - \sum_i a_i \rho_i \diamond g_i &= \mathbf{M}(f) + q - \sum_i a_i \mathbf{M}(g_i) * \rho_i - \sum_i h_i \\ &= \mathbf{M}(f) - \sum_i a_i \mathbf{M}(g_i) * \rho_i + h. \end{aligned}$$

Thus, setting  $\tau := \mathbf{T}(f) = \mathbf{T}(g_i) \circ \rho_i \in \mathcal{B}^{(m)}$ , we have  $\mathbf{T}(q) < \tau$  and  $\mathbf{T}(h_i) < \tau$  for each  $i$ , so that  $\mathbf{T}(h) < \tau$ .

Therefore  $\mathbf{M}(f) = \sum_i a_i \mathbf{M}(g_i) * \rho_i = \sum_i \mathbf{M}(a_i \rho_i \diamond g_i)$  implies  $f - \sum_i a_i \rho_i \diamond g_i = h$  so that  $\mathbf{T}(f - \sum_i a_i \rho_i \diamond g_i) = \mathbf{T}(h) < \mathbf{T}(f)$  proving (2)  $\implies$  (3).

Conversely,

$$\mathbf{T}\left(f - \sum_i a_i \rho_i \diamond g_i\right) < \mathbf{T}(f) \implies \mathbf{M}(f) - \sum_i a_i \mathbf{M}(g_i) * \rho_i = 0.$$

□

**Theorem 22.** For any set  $F \subset \mathcal{A}^m \setminus \{0\}$ , among the following conditions:

1.  $f \in \mathbb{I}_W(F) \iff$  it has a restricted strong Gröbner representation

$$f = \sum_{i=1}^{\mu} a_i g_i \star \rho_i = \sum_{i=1}^{\mu} a_i \rho_i \diamond g_i$$

in terms of  $F$  which further satisfies

$$\mathbf{T}(f) = \mathbf{T}(g_1) \circ \rho_1 > \cdots > \mathbf{T}(g_i) \circ \rho_i > \mathbf{T}(g_{i+1}) \circ \rho_{i+1};$$

2.  $f \in \mathbb{I}_W(F) \iff$  it has a restricted strong Gröbner representation in terms of  $F$ ;
3.  $F$  is a restricted strong Gröbner basis of  $\mathbb{I}_W(F)$ ;
4. for each  $f \in \mathcal{A}^m \setminus \{0\}$  and any restricted strong normal form  $h$  of  $f$  w.r.t.  $F$  we have  $f \in \mathbb{I}_W(F) \iff h = 0$ ;

5.  $f \in \mathbb{I}_W(F) \iff$  it has a restricted weak Gröbner representation in terms of  $F$ ;
6.  $F$  is a restricted weak Gröbner basis of  $\mathbb{I}_W(F)$ ;
7. for each  $f \in \mathcal{A}^m \setminus \{0\}$  and any restricted weak normal form  $h$  of  $f$  w.r.t.  $F$  we have  $f \in \mathbb{I}_W(F) \iff h = 0$ .

there are the implications

$$\begin{array}{ccccccc}
 (1) & \iff & (2) & \iff & (3) & \iff & (4) \\
 & & \Downarrow & & \Downarrow & & \Downarrow \\
 & & (5) & \iff & (6) & \iff & (7)
 \end{array}$$

If  $R$  is a skew field we have also the implication  $(5) \implies (2)$  and as a consequence the seven conditions are equivalent.

*Proof.* The implications  $(1) \implies (2) \implies (3)$ ,  $(5) \implies (6)$ ,  $(2) \implies (5)$ ,  $(3) \implies (6)$  and  $(4) \implies (7)$  are trivial.

Ad  $(3) \implies (1)$ : for each  $f \in \mathbb{I}_W(F)$  by assumption there are elements  $g \in F$ ,  $\rho \in \mathcal{B}$ ,  $a \in R \setminus \{0\}$ , such that

$$\mathbf{T}(f) = \mathbf{T}(g) \circ \rho \text{ and } \mathbf{M}(f) = a\mathbf{M}(g) * \rho.$$

Thus  $\mathbf{M}(a\rho \diamond \mathbf{M}(g)) = a\mathbf{M}(g) * \rho = \mathbf{M}(f)$  and denoting, for  $f = \mathbf{M}(f) + q$  and  $g = \mathbf{M}(g) + p$ ,

$$f_1 := f - a\rho \diamond g = q - \text{tail}(a\rho \diamond \mathbf{M}(g)) - a\rho \diamond p$$

we have  $\mathbf{T}(f_1) < \mathbf{T}(f)$  so the claim follows by induction, since  $\mathcal{B}^{(m)}$  is well-ordered by  $<$ .

Ad  $(6) \implies (5)$ : similarly, for each  $f \in \mathbb{I}_W(F)$  by assumption there are elements  $g_i \in F$ ,  $\rho_i \in \mathcal{B}$ ,  $a_i \in R \setminus \{0\}$  such that

- $\mathbf{T}(f) = \mathbf{T}(g_i) \circ \rho_i$  for all  $i$ ,
- $\mathbf{M}(f) = \sum_i a_i \mathbf{M}(g_i) * \rho_i = \sum_i a_i \rho_i \diamond \mathbf{M}(g_i)$ .

Thus  $\mathbf{T}(f - \sum_i a_i \rho_i \diamond g_i) < \mathbf{T}(f)$  and it is then sufficient to denote  $f_1 := f - \sum_i a_i \rho_i \diamond g_i$  in order to deduce the claim by induction.

Ad  $(3) \implies (4)$  and  $(6) \implies (7)$ : either

- $h = 0$  and  $f = f - h \in \mathbb{I}_W(F)$  or
- $h \neq 0$ ,  $\mathbf{M}(h) \notin \mathbf{M}_W(\mathbb{I}_W(F))$ ,  $h \notin \mathbb{I}_W(F)$  and  $f \notin \mathbb{I}_W(F)$ .

Ad  $(4) \implies (2)$  and  $(7) \implies (5)$ : for each  $f \in \mathbb{I}_W(F)$ , its normal form is  $h = 0$  and  $f = f - h$  has a strong (resp.: weak) Gröbner representation in terms of  $F$ .

Ad  $(5) \implies (2)$ : let  $f \in \mathbb{I}_W(F) \setminus \{0\}$ ; since  $R$  is a skew field, (5) implies the existence of elements  $g \in F$ ,  $\rho \in \mathcal{B}$ , such that  $\mathbf{T}(f) = \mathbf{T}(g) \circ \rho =: \tau$ ; thus denoting  $d \in R \setminus \{0\}$  the value which satisfies

$$d\tau = \mathbf{M}(\rho \diamond g) = \mathbf{M}(g) * \rho,$$



we have

$$\mathbf{M}(f) = \text{lc}(f)d^{-1}d\tau = \text{lc}(f)d^{-1}\mathbf{M}(g) * \rho = \mathbf{M}\left((\text{lc}(f)d^{-1})\rho \diamond g\right)$$

as required.  $\square$

## 8 Lifting Theorem for Restricted Modules

Given the finite set

$$F := \{g_1, \dots, g_u\} \subset \mathcal{A}^m, g_i = \mathbf{M}(g_i) - p_i =: a_i \tau_i \mathbf{e}_{l_i} - p_i,$$

let us now denote  $\mathbf{M}$  the restricted module  $\mathbf{M} := \mathbb{I}_W(F)$  endowed with its natural  $\Gamma$ -pseudovaluation  $\mathbf{T}(\cdot)$ .

Considering both the left  $R$ -module  $R \otimes_R \mathcal{A}^{\text{op}}$  and the left  $R$ -module  $R \otimes_R \mathcal{G}^{\text{op}}$ , which, as sets, coincide, we impose on the left  $R$ -module  $(R \otimes_R \mathcal{A}^{\text{op}})^u$ , whose canonical basis is denoted  $\{e_1, \dots, e_u\}$  and whose generic element has the shape

$$\sum_i a_i e_{l_i} \rho_i, \rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}, 1 \leq l_i \leq u,$$

the  $\Gamma^{(m)}$ -pseudovaluation – compatible with the natural  $\Gamma$ -pseudovaluation of  $\mathcal{A}$  –

$$w : (R \otimes_R \mathcal{A}^{\text{op}})^u \rightarrow \Gamma^{(m)}$$

defined for each  $\sigma := \sum_i a_i e_{l_i} \rho_i \in (R \otimes_R \mathcal{A}^{\text{op}})^u \setminus \{0\}$  as

$$w(\sigma) := \max_{<} \{\mathbf{T}(g_{l_i}) \circ \rho_i, \rho_i \in \mathcal{B}\} \in \Gamma^{(m)}$$

so that  $G((R \otimes_R \mathcal{A}^{\text{op}})^u) = (G(R \otimes_R \mathcal{A}^{\text{op}}))^u = (R \otimes_R \mathcal{G}^{\text{op}})^u$  and its corresponding  $\Gamma^{(m)}$ -homogeneous – of  $\Gamma^{(m)}$ -degree  $w(\sigma)$  – *leading form* is

$$\mathcal{L}(\sigma) := \sum_{h \in H} a_h e_{l_h} \rho_h \in (R \otimes_R \mathcal{G}^{\text{op}})^u \text{ where } H := \{h : \tau_{l_h} \circ \rho_h \mathbf{e}_{l_h} = w(\sigma)\}.$$

We can therefore consider the morphisms

$$\begin{aligned} \mathfrak{s}_W : (R \otimes_R \mathcal{G}^{\text{op}})^u &\rightarrow \mathcal{G}^m & \mathfrak{s}_W \left( \sum_i a_i e_{l_i} \rho_i \right) &:= \sum_i a_i \mathbf{M}(g_{l_i}) * \rho_i, \\ \mathfrak{S}_W : (R \otimes_R \mathcal{A}^{\text{op}})^u &\rightarrow \mathcal{A}^m & \mathfrak{S}_W \left( \sum_i a_i e_{l_i} \rho_i \right) &:= \sum_i a_i g_{l_i} \star \rho_i. \end{aligned}$$

We can equivalently reformulate this setting in terms of Weispfenning multiplication considering the morphisms

$$\begin{aligned} \mathfrak{s}_W : \mathcal{G}^u &\rightarrow \mathcal{G}^m & \mathfrak{s}_W \left( \sum_{i=1}^u \left( \sum_{\rho \in \mathcal{B}} a_{i\rho} \rho \right) e_i \right) &:= \sum_{i=1}^u \sum_{\rho \in \mathcal{B}} a_{i\rho} \mathbf{M}(g_i) * \rho, \\ \mathfrak{S}_W : \mathcal{A}^u &\rightarrow \mathcal{A}^m & \mathfrak{S}_W \left( \sum_{i=1}^u \left( \sum_{\rho \in \mathcal{B}} a_{i\rho} \rho \right) e_i \right) &:= \sum_{i=1}^u \sum_{\rho \in \mathcal{B}} a_{i\rho} \rho \diamond g_i, \end{aligned}$$

where the symbols  $\{e_1, \dots, e_u\}$  denote the common canonical basis of  $\mathcal{A}^u$  and  $\mathcal{G}^u$ , which, as sets, coincide and which satisfy  $\mathcal{G}^u = G(\mathcal{A})^u = G(\mathcal{A}^u)$  under the pseudovaluation  $w : \mathcal{A}^u \rightarrow \Gamma^{(m)}$  defined, for each

$$\sigma := \sum_{i=1}^u \left( \sum_{\rho \in \mathcal{B}} a_{i\rho} \rho \right) e_i \in \mathcal{A}^u \setminus \{0\}$$

by

$$w(\sigma) := \max_{<} \left\{ \mathbf{T}(g_i) \circ \rho : a_{i\rho} \neq 0 \right\} \in \Gamma^{(m)}.$$

The corresponding  $\Gamma^{(m)}$ -homogeneous – of  $\Gamma^{(m)}$ -degree  $w(\sigma)$  – *leading form* is

$$\mathcal{L}(\sigma) := \sum_{i=1}^u \left( \sum_{\rho \in B_i} a_{i\rho} \rho \right) e_i \in \mathcal{G}^u$$

where, for each  $i$  we set  $B_i := \{\rho \in \mathcal{B} : \mathbf{T}(g_i) \circ \rho = w(\sigma)\}$ .

**Definition 23.**

- if  $u \in \ker(\mathfrak{s}_W)$  is  $\Gamma^{(m)}$ -homogeneous and  $U \in \ker(\mathfrak{S}_W)$  is such that  $u = \mathcal{L}(U)$ , we say that  $u$  *lifts* to  $U$ , or  $U$  is a *lifting* of  $u$ , or simply  $u$  *has a lifting*;
- a restricted *Gebauer–Möller set* for  $F$  is any  $\Gamma^{(m)}$ -homogeneous basis of  $\ker(\mathfrak{s}_W)$ ;
- for each  $\Gamma^{(m)}$ -homogeneous element  $\sigma = \sum_i a_i e_{l_i} \rho_i \in (R \otimes_R \mathcal{A}^{\text{op}})^u$  – or, equivalently,

$$\sigma = \sum_{i=1}^u a_i \rho_i e_i \in \mathcal{A}^u \setminus \{0\}, a_i \neq 0, \implies \mathbf{T}(g_i) \circ \rho_i = w(\sigma),$$

we say that  $\mathfrak{S}_W(\sigma)$  has a restricted *quasi-Gröbner representation* in terms of  $F$  if it can be written as

$$\mathfrak{S}_W(\sigma) = \sum_{l=1}^{\mu} a_l g_l \star \rho_l = \sum_{l=1}^{\mu} a_l \rho_l \diamond g_l : \rho_l \in \mathcal{B}, a_l \in R \setminus \{0\}, g_l \in F$$

with  $w(\sigma) > \mathbf{T}(a_l g_l \star \rho_l) = \mathbf{T}(g_l) \circ \rho_l$  for each  $l$ , – or, equivalently,

$$\mathfrak{S}_W(\sigma) = \sum_{i=1}^u h_i \diamond g_i, h_i \in \mathcal{A}^u, w(\sigma) > \mathbf{T}(g_i) \circ \mathbf{T}(h_i).$$

- Denoting for each set  $S \subset \mathbf{M}$ ,  $\mathcal{L}\{S\} := \{\mathcal{L}(g) : g \in S\} \subset G(\mathbf{M})$ , a set  $B \subset \mathbf{M}$  is called a restricted *standard basis* of  $\mathbf{M}$  if

$$\mathbb{I}_W(\mathcal{L}\{B\}) = \mathbb{I}_W(\mathcal{L}\{\mathbf{M}\}).$$

□

**Theorem 24** (Möller–Pritchard). [22, 33, 34] *With the present notation and denoting  $\mathfrak{GM}_W(F)$  any restricted Gebauer–Möller set for  $F$ , the following conditions are equivalent:*

1.  $F$  is a restricted Gröbner basis of  $\mathbf{M}$ ;
2.  $f \in \mathbf{M} \iff f$  has a restricted Gröbner representation in terms of  $F$ ;
3. for each  $\sigma \in \mathfrak{GM}_W(F)$ , the restricted  $S$ -polynomial  $\mathfrak{S}_W(\sigma)$  has a restricted quasi-Gröbner representation  $\mathfrak{S}_W(\sigma) = \sum_{l=1}^{\mu} a_l \rho_l \diamond g_l = \sum_{l=1}^{\mu} a_l g_l \star \rho_l$ , in terms of  $F$ ;
4. each  $\sigma \in \mathfrak{GM}_W(F)$  has a lifting  $\text{lift}(\sigma)$ ;
5. each  $\Gamma^{(m)}$ -homogeneous element  $u \in \ker(\mathfrak{s}_W)$  has a lifting  $\text{lift}(u)$ .

*Proof.*

(1)  $\implies$  (2) is Theorem 22 (6)  $\implies$  (5).

(2)  $\implies$  (3)  $\mathfrak{S}_W(\sigma) \in \mathbf{M}$  and  $\mathbf{T}(\mathfrak{S}_W(\sigma)) < w(\sigma)$ .

(3)  $\implies$  (4) Let

$$\mathfrak{S}_W(\sigma) = \sum_{i=1}^{\mu} a_i \rho_i \diamond g_i = \sum_{i=1}^{\mu} a_i g_i \star \rho_i, w(\sigma) > \tau_{l_i} \circ \rho_i \mathbf{e}_{u_i}$$

be a restricted quasi-Gröbner representation in terms of  $F$ ; then

$$\text{lift}(\sigma) := \sigma - \sum_{i=1}^{\mu} a_i e_{l_i} \rho_i$$

is the required lifting of  $\sigma$ .

(4)  $\implies$  (5) Let

$$u := \sum_i a_i e_{l_i} \rho_i \in (R \otimes_R \mathcal{G}^{\text{op}})^u, \tau_{l_i} \circ \rho_i \mathbf{e}_{u_i} = w(u),$$

be a  $\Gamma^{(m)}$ -homogeneous element in  $\ker(\mathfrak{s}_W)$  of  $\Gamma^{(m)}$ -degree  $w(u)$ .

Then there are  $\rho_\sigma \in \mathcal{B}$ ,  $a_\sigma \in R \setminus \{0\}$ , for which

$$u = \sum_{\sigma \in \mathfrak{GM}_W(F)} a_\sigma \sigma * \rho_\sigma, w(\sigma) \circ \rho_\sigma = w(u).$$

For each  $\sigma \in \mathfrak{GM}_W(F)$  denote

$$\bar{\sigma} := \sigma - \text{lift}(\sigma) = \mathcal{L}(\text{lift}(\sigma)) - \text{lift}(\sigma) := \sum_{i=1}^{\mu_\sigma} a_{i\sigma} e_{l_{i\sigma}} \rho_{i\sigma} \in (R \otimes_R \mathcal{A}^{\text{op}})^u$$

and remark that  $\tau_{l_i} \circ \rho_{i\sigma} \mathbf{e}_{u_i} \leq w(\bar{\sigma}) < w(\sigma)$  and  $\mathfrak{S}_W(\bar{\sigma}) = \mathfrak{S}_W(\sigma)$ .

It is sufficient to define

$$\text{lift}(u) := \sum_{\sigma \in \mathfrak{M}_W(F)} a_\sigma \text{lift}(\sigma) \star \rho_\sigma = \sum_{\sigma \in \mathfrak{M}_W(F)} a_\sigma \rho_\sigma \diamond \text{lift}(\sigma)$$

and

$$\bar{u} := \sum_{\sigma \in \mathfrak{M}_W(F)} a_\sigma \bar{\sigma} \star \rho_\sigma = \sum_{\sigma \in \mathfrak{M}_W(F)} a_\sigma \rho_\sigma \diamond \bar{\sigma}$$

to obtain

$$\text{lift}(u) = u - \bar{u}, \mathcal{L}(\text{lift}(u)) = u, \mathfrak{S}_W(\bar{u}) = \mathfrak{S}_W(u), \mathfrak{S}_W(\text{lift}(u)) = 0.$$

- (5)  $\implies$  (1) Let  $g \in \mathbf{M}$ , so that there are  $\rho_i \in \mathcal{B}, a_i \in R \setminus \{0\}, 1 \leq i \leq u$ , such that  $\sigma_1 := \sum_{i=1}^\mu a_i e_{l_i} \rho_i \in (R \otimes_R \mathcal{A}^{\text{op}})^u$  satisfies

$$g = \mathfrak{S}_W(\sigma_1) = \sum_{i=1}^\mu a_i g_{l_i} \star \rho_i = \sum_{i=1}^\mu a_i \rho_i \diamond g_{l_i}.$$

Denoting  $H := \{i : \mathbf{T}(g_{l_i}) \circ \rho_i = \tau_{l_i} \circ \rho_i \mathbf{e}_{u_{l_i}} = w(\sigma_1)\}$ , then either

- $w(\sigma_1) = \mathbf{T}(g) \in \mathcal{B}^{(m)}$  so that, for each  $i \in H$ ,  $\mathbf{M}(a_i \mathbf{M}(g_{l_i}) \star \rho_i) = a_i \mathbf{M}(g_{l_i}) * \rho_i$  and

$$\mathbf{M}(g) = \sum_{i \in H} a_i \mathbf{M}(g_{l_i}) * \rho_i \in \mathbf{M}\{\mathbb{I}_W(\mathbf{M}\{F\})\},$$

and we are through, or

- $\mathbf{T}(g) < w(\sigma_1)$ , in which case<sup>1</sup>  $0 = \sum_{i \in H} a_i \mathbf{M}(g_{l_i}) * \rho_i = \mathfrak{s}_W(\mathcal{L}(\sigma_1))$  and the  $\Gamma^{(m)}$ -homogeneous element  $\mathcal{L}(\sigma_1) \in \ker(\mathfrak{s}_W)$  has a lifting

$$U := \mathcal{L}(\sigma_1) - \sum_{j=1}^v a_j e_{l_j} \rho_j \in (R \otimes_R \mathcal{A}^{\text{op}})^u$$

with

$$\sum_{j=1}^v a_j \rho_j \diamond g_{l_j} = \sum_{i \in H} a_i \rho_i \diamond g_{l_i} \text{ and } \tau_{l_j} \circ \rho_j \mathbf{e}_{u_{l_j}} < w(\sigma_1)$$

so that  $g = \mathfrak{S}_W(\sigma_2)$  and  $w(\sigma_2) < w(\sigma_1)$  for

$$\sigma_2 := \sum_{i \notin H} a_i e_{l_i} \rho_i + \sum_{j=1}^v a_j e_{l_j} \rho_j \in (R \otimes_R \mathcal{A}^{\text{op}})^u$$

and the claim follows by the well-orderedness of  $<$ .

□

**Theorem 25** (Janet—Schreier). [17, 38, 39]

*With the same notation the equivalent conditions (1-5) imply that*

---

<sup>1</sup>Compare Remark 15.

6.  $\{\text{lift}(\sigma) : \sigma \in \mathfrak{M}_W(F)\}$  is a restricted standard basis of  $\ker(\mathfrak{S}_W)$ .

*Proof.* Let  $\sigma_1 := \sum_{i=1}^{\mu} a_i e_{l_i} \rho_i \in \ker(\mathfrak{S}_W) \subset (R \otimes_R \mathcal{A}^{\text{op}})^u$ .

Denoting  $H := \{i : \tau_{l_i} \circ \rho_i e_{l_i} = w(\sigma_1)\}$ , we have

$$\mathcal{L}(\sigma_1) = \sum_{i \in H} a_i e_{l_i} \rho_i \in \ker(\mathfrak{s}_W)$$

and there is a  $\Gamma^{(m)}$ -homogeneous representation

$$\mathcal{L}(\sigma_1) = \sum_{\sigma \in \mathfrak{M}_W(F)} a_{\sigma} \sigma * \rho_{\sigma}, w(\sigma) \circ \rho_{\sigma} = w(\sigma_1)$$

with  $\rho_{\sigma} \in \mathcal{B}, a_{\sigma} \in R \setminus \{0\}$ .

Then

$$\begin{aligned} \sigma_2 &:= \sigma_1 - \sum_{\sigma \in \mathfrak{M}_W(F)} a_{\sigma} \rho_{\sigma} \diamond \text{lift}(\sigma) \\ &= \sigma_1 - \sum_{\sigma \in \mathfrak{M}_W(F)} a_{\sigma} \rho_{\sigma} \diamond (\sigma - \bar{\sigma}) \\ &= \sigma_1 - \mathcal{L}(\sigma_1) + \sum_{\sigma \in \mathfrak{M}_W(F)} a_{\sigma} \rho_{\sigma} \diamond \bar{\sigma} \\ &= \sum_{i \notin H} a_i e_{l_i} \rho_i + \sum_{\sigma \in \mathfrak{M}_W(F)} \sum_{i=1}^{\mu_{\sigma}} (a_{\sigma} a_{i\sigma}) e_{l_{i\sigma}} (\rho_{i\sigma} \star \rho_{\sigma}) \end{aligned}$$

satisfies both  $\sigma_2 \in \ker(\mathfrak{S}_W)$  and  $w(\sigma_2) < w(\sigma_1)$ ; thus the claim follows by induction.  $\square$

## 9 Weispfenning: Restricted Representation and Completion

Note that  $R$  is effectively given as a quotient of a free monoid ring  $\mathcal{R} := \mathbb{D}\langle \bar{\mathbf{v}} \rangle$  over  $\mathbb{D}$  and the monoid  $\langle \bar{\mathbf{v}} \rangle$  of all words over the alphabet  $\bar{\mathbf{v}}$  modulo a bilateral ideal  $I, R = \mathcal{R}/I$ .

Wlog we will assume that  $<$  orders the set  $\bar{\mathbf{v}}$  so that  $X_1 < X_2 < \dots$  and that its restriction to  $\langle \bar{\mathbf{v}} \rangle$  is a sequential term-ordering, *id est* the set  $\{\omega \in \langle \bar{\mathbf{v}} \rangle : \omega < \tau\}$  is finite for each  $\tau \in \langle \bar{\mathbf{v}} \rangle$ .

Note that, under these assumptions, (1) implies the existence in  $\mathcal{A}$  of relations

$$X_i \star d = \sum_{l=1}^i a_{li}(d) X_l + a_{0i}(d), a_{li}(d) \in \mathbb{D}\langle \bar{\mathbf{v}} \rangle, \text{ for each } X_i \in \bar{\mathbf{v}}, d \in R \setminus \{0\}$$

and

$$\rho \star x_j = \sum_{\substack{v \in \mathcal{B} \\ v \leq \rho}} a_{\rho j v} v, a_{\rho j v} \in \mathbb{D}\langle \bar{\mathbf{v}} \rangle, \text{ for each } x_j \in \bar{\mathbf{v}}, \rho \in \mathcal{B}.$$

**Lemma 26.** [44] *Let*

$$F := \{g_1, \dots, g_u\} \subset \mathcal{A}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{i_i} - p_i;$$

set  $\Omega := \max_{<} \{\mathbf{T}(g_i) : 1 \leq i \leq u\}$ .

Let  $\mathbf{M}$  be the bilateral module  $\mathbf{M} := \mathbb{I}_2(F)$  and  $\mathbb{I}_W(F)$  the restricted module

$$\begin{aligned} \mathbb{I}_W(F) &:= \text{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F) \\ &= \text{Span}_R(a\rho \diamond f : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F). \end{aligned}$$

If every  $g \star a_{\rho_{jv}}, x_j \in \bar{\mathbf{v}}, v, \rho \in \mathcal{B}, v \leq \rho < \Omega$ , has a restricted representation in terms of  $F$  w.r.t. a sequential term-ordering  $<$ , then every  $g \star r, g \in F, r \in \mathcal{A}$ , has a restricted representation in terms of  $F$  w.r.t.  $<$ .

*Proof.* We can wlog assume  $r = \prod_{l=1}^v x_{j_l}, x_{j_l} \in \bar{\mathbf{v}}$  and prove the claim by induction on  $v \in \mathbb{N}$ .

Thus we have a restricted representation in terms of  $F$

$$g \star \left( \prod_{l=1}^{v-1} x_{j_l} \right) = \sum_h d_h g_{i_h} \star \rho_h, \tau_{i_h} \circ \rho_h \leq \mathbf{T}(g) \circ \prod_{l=1}^v x_{j_l},$$

whence we obtain

$$\begin{aligned} g \star \prod_{l=1}^v x_{j_l} &= \left( g \star \prod_{i=1}^{v-1} x_{j_i} \right) \star x_{j_v} \\ &= \left( \sum_h d_h g_{i_h} \star \rho_h \right) \star x_{j_v} \\ &= \sum_h d_h g_{i_h} \star (\rho_h \star x_{j_v}) \\ &= \sum_h d_h g_{i_h} \star \left( \sum_{\substack{v \in \mathcal{B} \\ v \leq \rho_h}} a_{\rho_h j_v} v \right) \\ &= \sum_h d_h \sum_{\substack{v \in \mathcal{B} \\ v \leq \rho_h}} (g_{i_h} \star a_{\rho_h j_v} v) v \end{aligned}$$

and since  $v \leq \rho_h < \mathbf{T}(f) \leq \Omega$  each element  $g_{i_h} \star a_{\rho_h j_v} v$  can be substituted with its restricted representation whose existence is granted by assumption.  $\square$

**Lemma 27.** [44] *Under the same assumption, if, for each  $g \in F$ , both each  $X_i \star g, X_i \in \bar{\mathbf{v}}$  and each  $g \star a_{\rho_{jv}}, x_j \in \bar{\mathbf{v}}, v, \rho \in \mathcal{B}, v \leq \rho < \Omega$ , have a restricted representation in terms of  $F$  w.r.t.  $<$ , then  $\mathbb{I}_W(F) = \mathbf{M}$ .*

*Proof.* It is sufficient to show that, for each  $f \in \mathbb{I}_W(F)$ , both each  $X_i \star f \in \mathbb{I}_W(F), X_i \in \bar{\mathbf{v}}$  and each  $f \star x_j \in \mathbb{I}_W(F), x_j \in \bar{\mathbf{v}}$ .

By assumption  $f = \sum_h d_h g_{i_h} \star \rho_h$ ,  $d_h \in R \setminus \{0\}$ ,  $\rho_h \in \mathcal{B} \subset \langle \overline{\mathbf{Z}} \rangle$ ,  $1 \leq i_h \leq u$ , so that

$$\begin{aligned} X_i \star f &= \sum_h (X_i \star d_h) g_{i_h} \star \rho_h \\ &= \sum_h \left( \sum_{l=1}^i a_{li}(d_h) X_l + a_{0i}(d_h) \right) g_{i_h} \star \rho_h \\ &= \sum_h \sum_{l=1}^i a_{li}(d_h) (X_l \star g_{i_h}) \star \rho_h + \sum_h a_{0i}(d_h) g_{i_h} \star \rho_h \end{aligned}$$

and

$$\begin{aligned} f \star x_j &= \sum_h d_h g_{i_h} \star (\rho_h \star x_j) \\ &= \sum_h d_h g_{i_h} \star \left( \sum_{\substack{v \in \mathcal{B} \\ v \leq \rho_h}} a_{\rho_h j v} v \right) \\ &= \sum_h d_h \sum_{\substack{v \in \mathcal{B} \\ v \leq \rho_h}} (g_{i_h} \star a_{\rho_h j v}) v \end{aligned}$$

and, since  $v \leq \rho_h < \mathbf{T}(f) \leq \Omega$  each element  $g_{i_h} \star a_{\rho_h j v}$  can be substituted with its restricted representation whose existence is granted by assumption.

The same holds for each  $X_l \star g_{i_h}$  thus the claim follows.  $\square$

**Corollary 28.** [44] *Let*

$$F := \{g_1, \dots, g_u\} \subset \mathcal{A}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{i_i} - p_i.$$

*Let  $\mathbf{M}$  be the bilateral module  $\mathbf{M} := \mathbb{I}_2(F)$  and  $\mathbb{I}_W(F)$  the restricted module*

$$\begin{aligned} \mathbb{I}_W(F) &:= \text{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F) \\ &= \text{Span}_R(a\rho \diamond f : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F). \end{aligned}$$

*$F$  is the bilateral Gröbner basis of  $\mathbf{M}$  iff*

1. *denoting  $\mathfrak{GM}(F)$  any restricted Gebauer–Möller set for  $F$ , each  $\sigma \in \mathfrak{GM}(F)$  has a restricted quasi-Gröbner representation in terms of  $F$ ;*
2. *for each  $g \in F$ , both  $X_i \star g$ ,  $X_i \in \overline{\mathbf{V}}$  and each*

$$g \star a_{\rho j v}, x_j \in \overline{\mathbf{v}}, v, \rho \in \mathcal{B}, v \leq \rho < \Omega,$$

*have a restricted representation in terms of  $F$  w.r.t.  $<$ .*

## 10 Finiteness, Noetherianity, Termination

Even if we restrict ourselves to a case in which both  $\bar{\mathbf{v}}$  and  $\bar{\mathbf{V}}$  are finite and that  $<$  is a sequential term-ordering on  $\langle \bar{\mathbf{Z}} \rangle$  so that the tests required by Corollary 28 are finitely many, unless we know and explicitly use noetherianity of  $\mathcal{A}$ , it is well-established that the best one can hope to be able of producing is a procedure which receiving as input a finite set of elements  $F := \{g_1, \dots, g_u\} \subset \mathcal{A}^m$  defining the module  $\mathbb{I}(F)$

- in case  $\mathbb{I}(F)$  has a finite (left, right, restricted, bilateral) Gröbner basis, halts returning such a finite Gröbner basis;
- otherwise, it produces an infinite sequence of elements

$$g_1, \dots, g_u, g_{u+1}, \dots, g_i, \dots$$

such that the infinite set  $\{g_i : i \in \mathbb{N}\}$  is a Gröbner basis of  $\mathbb{I}(F)$ .

A nice and efficient procedure to this aim has been proposed by Pritchard [34], [26, IV.47.7]; with slight modification Pritchard's approach allows also to produce

- a procedure, which, given further an element  $g \in \mathcal{A}^m$ , terminates if and only if  $g \in \mathbb{I}(F)$  in which case it produces also a Gröbner representation of it;
- a procedure, which, given an element  $g \in \mathcal{A}^m$  and any subset  $\mathcal{N} \subset \mathbf{N}(\mathbb{I}(F))$ , terminates if and only if  $g \in \mathbb{I}(F)$  has a canonical representation

$$\mathbf{Rep}(g, \mathbb{I}(F)) \subset \text{Span}_{\mathbb{D}}(\mathcal{N})$$

in which case it produces such canonical representation, thus granting the impossibility of using non-commutative Gröbner bases as a cryptographical tool.

The procedures, assuming  $<$  to be sequential, consists in fixing an enumerated set

$$v_1, v_2, \dots, v_i, v_{i+1}, \dots$$

of the elements of  $\langle \bar{\mathbf{Z}} \rangle^{(m)}$  which satisfy

- $v_i < v_{i+1}$  for each  $i$ ,
- for each  $v \in \langle \bar{\mathbf{Z}} \rangle^{(m)}$  there is a value  $i : v < v_i$ ;

and denotes, for each  $i \in \mathbb{N}$

$$\mathbf{S}_i := \{v \leq v_i\} \subset \mathbf{S}^{(m)}$$

Then we set  $G_0 := G, i := 1, S_0 := \emptyset$  and iteratively we compute

- $B_i := \{\sigma \in \mathbb{G}\mathbb{M}(G_{i-1}), w(\sigma) \leq v_i\}$ ,
- $G_i := G_{i-1} \cup \{\text{NF}(\mathfrak{S}(\sigma), G_{i-1}) : \sigma \in B_i\}$ .



## 11 Restricted Gröbner basis

In order to compute a restricted Gröbner basis we need to formulate Spear Theorem in the restricted setting.

It is more convenient to consider the ring  $\mathcal{Q}/I$  and the obvious projections

$$\Phi : (\mathcal{Q}/I)^m \twoheadrightarrow \mathcal{A}^m, \ker(\Phi) = (I/I)^m = \mathbb{I}_2 \left( \pi(H)^{(m)} \right)$$

where  $H = G \setminus (G_0 \cup C)$  and  $\pi(H)^{(m)} := \{\pi(h)\mathbf{e}_j, h \in H, 1 \leq j \leq m\}$ .

Then given a restricted module  $\mathbf{M} := \mathbb{I}_W(F) \subset \mathcal{A}^m$ , where  $F \subset \mathbf{Zach}_{<}(\mathcal{A})^{(m)} \subset \mathcal{Q}^{(m)}$  and wlog  $f = \Pi(f)$  for each  $f \in F$ , we consider the restricted module

$$\begin{aligned} \mathbf{M}' &:= \mathbf{M} + \text{Span}_R \left( \gamma v f \star \rho : \gamma \in \mathbb{D} \setminus \{0\}, v \in \langle \bar{\mathbf{v}} \rangle, \gamma v \notin \mathbf{M}(I), \rho \in \langle \bar{\mathbf{v}} \rangle, f \in F \cup \pi(H)^{(m)} \right) \\ &= \mathbf{M} + \text{Span}_R \left( \gamma v \rho \diamond f : \gamma \in \mathbb{D} \setminus \{0\}, v \in \langle \bar{\mathbf{v}} \rangle, \gamma v \notin \mathbf{M}(I), \rho \in \langle \bar{\mathbf{v}} \rangle, f \in F \cup \pi(H)^{(m)} \right). \end{aligned}$$

**Lemma 29** (Spear). [40],[26, II.Proposition 24.7.3., IV.Theorem 50.6.3.(1)] *With the present notation if  $F$  is a reduced restricted Gröbner basis of  $\mathbf{M}'$ , then*

$$\{g \in F : g = \Phi(g)\} = \{\Phi(g) : g \in F, \mathbf{T}(g) \in \mathcal{B}^{(m)}\} = F \cap \mathbf{Zach}_{<}(\mathcal{A})^m$$

*is a reduced restricted Gröbner basis of  $\mathbf{M}$ .*

*Proof.* Let  $m \in \mathbf{M}$  and  $m' \in \mathbf{M}' \cap \mathbf{Zach}_{<}(\mathcal{A})^m \subset \mathcal{Q}^m$  be such that  $\Phi(m') = m$ , so that  $\mathbf{M}(m') = \mathbf{M}(m) \notin \mathbf{M}(I^m)$ , and  $m' = \pi(m')$ .

Then there are  $g_i \in F$ ,  $\rho_i \in \bar{\mathbf{v}}$ ,  $\bar{v}_i \in \langle \bar{\mathbf{v}} \rangle$ ,  $\gamma_i \in \mathbb{D} \setminus \{0\}$ ,  $\gamma_i \bar{v}_i \notin \mathbf{M}(I)$  such that, denoting  $\mathbf{M}(g_i) = c_i \tau_i \mathbf{e}_{\iota_i} = c_i v_i \omega_i \mathbf{e}_{\iota_i}$ , satisfy

- $\mathbf{M}(m) := c \tau \mathbf{e}_{\iota} = c v \omega \mathbf{e}_{\iota} = \sum_i \gamma_i \bar{v}_i \mathbf{M}(g_i) \star \rho_i$ ,
- $\tau = \bar{v}_i \cdot \tau_i \cdot \rho_i$ ,
- $\omega = \omega_i \circ \rho_i$ ,
- $\iota_i = \iota$ ,
- $\Pi(g_i) = g_i$  and  $\mathbf{T}(g_i) \in \mathcal{B}^{(m)}$ .

Thus in particular we have

- $\mathbf{T}(m) = \mathbf{T}(g_i) \circ \rho_i$  and
- $\mathbf{M}(m) = \sum_i \gamma_i \bar{v}_i \mathbf{M}(g_i) \star \rho_i = \sum_i \gamma_i \bar{v}_i \rho_i \diamond \mathbf{M}(g_i)$

as required. □

Let  $F \subset \mathcal{A}^m$  and express each  $g \in F$  as

$$g = \mathbf{M}(g) - p_g =: c_g \omega_g \mathbf{e}_{\iota_g} - p_g = (\gamma_g v_g - \chi_g) \omega_g \mathbf{e}_{\iota_g} - p_g$$

with

$$p_g \in \mathcal{A}^m, c_g \in R, \omega_g \in \langle \bar{\mathbf{V}} \rangle, \chi_g \in R, \gamma_g \in \mathbb{D}, v_g \in \langle \bar{\mathbf{V}} \rangle,$$

and  $\mathbf{T}(p_g) < \tau_g, \gamma_g v_g \notin \mathbf{M}(I)$  and  $\mathbf{T}(\chi_g) < v_g$ .

Note that, analogously, for each  $h \in H := G \setminus \{G_0 \cup C\} \subset Q$ ,  $\mathbf{M}(h)$  can be uniquely expressed as

$$\mathbf{M}(h) = c_h \omega_h = (\gamma_h v_h + \chi_h) \omega_h$$

with  $\gamma_h \in \mathbb{D}, v_h \in \langle \bar{\mathbf{V}} \rangle, \omega_h \in \langle \bar{\mathbf{V}} \rangle, c_h, \chi_h \in R, \gamma_h v_h \notin \mathbf{M}(I), \mathbf{T}(\chi_h) < v_h$ .

In order to apply Spear's Theorem we adapt the notation of [23, Corollary 14] and consider

- the module  $(Q/I)^{|F|+m|H|}$  indexed by the set  $F \cup \pi(H)^{(m)}$  and whose canonical basis is denoted  $\{\mathbf{e}(f) : f \in F \cup \pi(H)^{(m)}\}$ , and
- $\hat{\mathfrak{S}}_2 : (Q/I)^{|F|+m|H|} \rightarrow \mathcal{A}^m : \mathbf{e}(h) \mapsto \Phi(h)$ , for each  $h \in F \cup G^{(m)}$ .

Spear's Theorem having reduced the problem of computing restricted Gebauer-Möller sets to the classical problem of computing Gebauer-Möller sets for elements in  $Q$  with a restricted representation, we can on one side use the classical Buchberger Theory for Free Associative Algebras and, on the other side, take advantage of the restricted shape of the terms.

In particular, among two terms  $v_1 \omega_1, v_2 \omega_2$  there is at most a single match and (by left and right cancellativity) either  $\omega_1 \mid_L \omega_2$  or  $\omega_2 \mid_L \omega_1$  and either  $v_1 \mid_R v_2$  or  $v_2 \mid_R v_1$ .

Thus, for

$$g_1, g_2 \in F, h \in H, \mathbf{M}(g_1) = \gamma_1 v_1 \omega_1 \mathbf{e}_{i_1}, \mathbf{M}(g_2) = \gamma_2 v_2 \omega_2 \mathbf{e}_{i_2}, \mathbf{M}(h) = \gamma_3 v_3 \omega_3, \omega_1 \mid_L \omega_2$$

with  $\gamma_i \in \mathbb{D}, v_i \in \langle \bar{\mathbf{V}} \rangle, \omega_i \in \langle \bar{\mathbf{V}} \rangle, \gamma_i v_i \notin \mathbf{M}(I)$  and

$$\iota_1 = \iota_2, \omega_1 \mid_L \omega_2, \omega_1 \rho = \omega_2, \rho \in \mathcal{B} :$$

A.1). if  $\omega_1 \mid_L \omega_3, \omega_1 \rho = \omega_3, \rho \in \mathcal{B}$  and  $v_3 \mid_R v_1, \lambda v_3 = v_1, \lambda \in \langle \bar{\mathbf{V}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \lambda \notin \mathbf{M}(I)$  we set

$$B(g_1, h) = \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \lambda \mathbf{e}(h) \mathbf{e}_{i_1} - \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \rho \diamond \mathbf{e}(g_1);$$

A.2). if  $\omega_3 \mid_L \omega_1, \omega_3 \rho = \omega_1, \rho \in \mathcal{B}$  and  $v_1 \mid_R v_3, \lambda v_1 = v_3, \lambda \in \langle \bar{\mathbf{V}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \lambda \notin \mathbf{M}(I)$  we set

$$B(g_1, h) = \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \rho \diamond \mathbf{e}(h) \mathbf{e}_{i_1} - \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \lambda \mathbf{e}(g_1);$$

A.3). if  $\omega_1 \mid_L \omega_3, \omega_1 \rho = \omega_3, \rho \in \mathcal{B}$  and  $v_1 \mid_R v_3, \lambda v_1 = v_3, \lambda \in \langle \bar{\mathbf{V}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \lambda \notin \mathbf{M}(I)$  we set

$$B(g_1, h) = \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \mathbf{e}(h) \mathbf{e}_{i_1} - \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \lambda \rho \diamond \mathbf{e}(g_1);$$

A.4). if  $\omega_3 \mid_L \omega_1, \omega_3 \rho = \omega_1, \rho \in \mathcal{B}$  and  $v_3 \mid_R v_1, \lambda v_3 = v_1, \lambda \in \langle \bar{\mathbf{V}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \lambda \notin \mathbf{M}(I)$  we set

$$B(g_1, h) = \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_3} \lambda \rho \diamond \mathbf{e}(h) \mathbf{e}_{i_1} - \frac{\text{lcm}(\gamma_1, \gamma_3)}{\gamma_1} \mathbf{e}(g_1);$$

B.1). if  $\omega_1 \mid_L \omega_2, \omega_1 \rho = \omega_2, \rho \in \mathcal{B}$  and  $v_2 \mid_R v_1, \lambda v_2 = v_1, \lambda \in \langle \bar{\mathbf{v}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_2} \lambda \notin \mathbf{M}(I)$   
we set

$$B(g_1, g_2) = \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_2} \lambda \mathbf{e}(g_2) - \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_1} \rho \diamond \mathbf{e}(g_1);$$

B.3). if  $\omega_1 \mid_L \omega_2, \omega_1 \rho = \omega_2, \rho \in \mathcal{B}$  and  $v_1 \mid_R v_2, \lambda v_1 = v_2, \lambda \in \langle \bar{\mathbf{v}} \rangle, \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_1} \lambda \notin \mathbf{M}(I)$   
we set

$$B(g_1, g_2) = \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_2} \mathbf{e}(g_2) - \frac{\text{lcm}(\gamma_1, \gamma_2)}{\gamma_1} \lambda \rho \diamond \mathbf{e}(g_1).$$

**Corollary 30.** *The set*

$$\{B(f, g) : f, g \in F, \iota_f = \iota_g, \omega_f \mid_L \omega_g\} \cup \{B(f, h) : f \in F, h \in H\}$$

*is a restricted Gebauer-Möller set.*

## 12 Strong restricted Gröbner basis

According Zacharias approach [47], modules in  $\mathcal{A}$  have (left/right/bilateral/restricted) strong Gröbner bases if and only if  $R$  is a (left/right/bilateral/restricted) strong ring [27], *id est* each (left/right/bilateral/restricted) ideal  $I \subset R$  has a strong basis.

Thus, under this assumption, from a restricted Gröbner basis  $F \subset \mathcal{A}^m$  of the restricted module  $\mathbb{I}_W(F)$ , we can obtain a strong restricted Gröbner basis of  $\mathbb{I}_W(F)$ , as follows.

For each  $g \in F$ , let us denote

- $H_g := \{h \in F \cup H^{(m)} : \omega_h \mid_L \omega_g\}$ ,
- for each  $h \in H_g, t_{hg} \in \langle \bar{\mathbf{v}} \rangle : \omega_h t_{hg} = \omega_g$ ,
- $J_g := \mathbb{I}_L(\text{lc}(h) : h \in H_g) \subset R$ ,
- $\{d_j, j \in J\}, d_j = \sum_{h \in H_g} \gamma_{jh} \text{lc}(h)$ , a strong left basis of  $J_g$ ,
- $S_g := \{\sum_{h \in H_g} \Pi(\gamma_{jh} t_{hg}) \diamond h, j \in J\}$ .

**Corollary 31.**  $\cup_{g \in F} S_g$  *is a strong restricted Gröbner representation in terms of*  $F$ .

## Acknowledgements

The senior author was partially supported by GNSAGA (INdAM, Italy).

## References

- [1] Apel J., *Computational ideal theory in finitely generated extension rings*, Theor. Comp. Sci. **224** (2000), 1–33
- [2] Becker T., Weispfenning V., *Gröbner Bases*, Springer (1991)

- [3] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Thesis, Innsbruck (1965)
- [4] Buchberger B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystem*, Aeq. Math. **4** (1970), 374–383
- [5] Buchberger B., *A Criterion for Detecting Unnecessary Reduction in the Construction of Gröbner bases*, L. N. Comp. Sci **72** (1979), 3–21, Springer
- [6] Buchberger, B. *Miscellaneous Results on Groebner Bases for Polynomial Ideals II*. Technical Report 83/1, University of Delaware, Department of Computer and Information Sciences, 1983. p. 31
- [7] Buchberger B., *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in Bose N.K. (Ed.) *Multidimensional Systems Theory* (1985), 184–232, Reider
- [8] J. Bueso, J. Gomez-Torrecillas, and A. Verschoren. *Methods in Non-Commutative Algebra* (2003). Kluwer
- [9] Ceria, M., Mora, T., *Buchberger-Zacharias Theory of Multivariate Ore Extensions*, J. P.A.A submitted
- [10] Dubé, T.W., *The Structure of Polynomial Ideals and Gröbner Bases*. SIAM J. Comput., **19**(4) (2006), 750–773
- [11] Gebauer R., Möller H.M., *On an Installation of Buchberger’s Algorithm*, J. Symb. Comp. **6**, (1988), 275–286
- [12] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, “*One sugar cube, please*”; or: *Selection strategies in Buchberger algorithm*, Proc. ISSAC ’91, (1991), 49–54, ACM
- [13] Hironaka, H. *Idealistic exponents of singularity* In: *Algebraic Geometry, The Johns Hopkins Centennial Lectures* (1977) 52-125
- [14] Hermann G., *Die Frage der endlich vielen Schritte in die Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788
- [15] Kandri-Rody, A., Weispfenning, W., *Non-commutative Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9** (1990), 1–26
- [16] Kredel H., *Solvable Polynomial rings* Dissertation, Passau (1992)
- [17] Janet M. , *Sur les systèmes d’équations aux dérivées partielles*, J. Math. Pure et Appl., **3** (1920), 65–151
- [18] Janet M., *Les systèmes d’équations aux dérivées partielles*, Mémoires Sci. Math. **XXI** (1927), Gauthiers-Villars.

- [19] Logar A., *Constructions over localizations of rings*, La Matematiche **42** (1987), 131–150
- [20] K. Madlener, B. Reinert, *String Rewriting and Gröbner bases – A General Approach to Monoid and Group Rings*, Progress in Computer Science and Applied Logic **15** (1991), 127–180, Birkhäuser
- [21] K. Madlener, B. Reinert, *Computing Gröbner bases in monoid and group rings*, Proc.ISSAC '93, ACM (1993), 254–263
- [22] Möller H.M., *On the construction of Gröbner bases using syzygies*, J. Symb. Comp. **6** (1988), 345–359
- [23] F. Mora, *De Nugis Groebnerialium 4: Zacharias, Spears, Möller* Proc. ISSAC'15 (2015), 191–198, ACM
- [24] T. Mora, *Seven variations on standard bases*, (1988)  
<ftp://ftp.disi.unige.it/person/MoraF/PUBLICATIONS/7Variations.tar.gz>
- [25] T. Mora, *Groebner bases in non-commutative algebras* L. N. Comp. Sci **358** (1989), 150–161, Springer
- [26] T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016)
- [27] T. Mora, *Zacharias Representation of Effective Associative Rings*, J. Symb. Comp. (submitted)
- [28] T. Mora, *A primer on ideal theoretical operation in non-commutative polynomial rings* J. Algebra Appl. **14**: 1550018 (2015)
- [29] Mosteig E., Sweedler M. *Valuations and filtrations*, J. Symb. Comp. **34** (2002), 399–435
- [30] Pesch M., *Gröbner Bases in Skew Polynomial Rings* Dissertation, Passau (1997)
- [31] Pesch M., *Two-sided Gröbner bases in Iterated Ore Extensions*, Progress in Computer Science and Applied Logic **15** (1991), 225–243, Birkhäuser
- [32] Pommaret J. F., *Systems of partial differential equations and Lie pseudogroups*, Gordon and Brach (1978)
- [33] Pritchard F. L., *A syzygies approach to non-commutative Gröbner bases*, Preprint (1994)
- [34] Pritchard F. L., *The ideal membership problem in non-commutative polynomial rings*, J. Symb. Comp. **22** (1996), 27–48
- [35] Reinert B., *A systematic Study of Gröbner Basis Methods*, Habilitation, Kaiserslautern (2003)

- [36] Reinert B., *Gröbner Bases in Function Ring – A Guide for Introducing Reduction Relations to Algebraic Structures*, J. Symb. Comp. J. Symb. Comp. **41** (2006), 1264–94
- [37] Rosenmann A., *An Algorithm for constructing Gröbner and free Schreier bases in free group algebras*, J. Symb. Comp. **16** (1993), 523–549
- [38] Schreyer F.O., *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionsatz*, Diplomarbeit, Hamburg (1980)
- [39] Schreyer F.O., *A standard basis approach to syzygies of canonical curves*, J. Reine angew. Math. **421** (1991), 83–123
- [40] Spear D.A., *A constructive approach to commutative ring theory*, in *Proc. of the 1977 MACSYMA Users' Conference*, NASA CP-2012 (1977), 369–376
- [41] Sweedler M., *Ideal bases and valuation rings*, Manuscript (1986) available at <http://math.usask.ca/fvk/Valth.html>
- [42] Szekeres L., *A canonical basis for the ideals of a polynomial domain*, Am. Math. Monthly **59** (1952), 379–386
- [43] Traverso C., Donato L., *Experimenting the Gröbner basis algorithm with APLI system*, Proc. ISSAC '89, (1989), 192–198, ACM
- [44] Weispfenning V., *Finite Gröbner bases in non-noetherian Skew Polynomial Rings* Proc. ISSAC'92 (1992), 320–332, A.C.M.
- [45] Wiesinger-Widi M., *Groebner Bases and Generalized Sylvester Matrices*. Ph.D. Thesis, Johannes Kepler University, Institute for Symbolic Computation, submitted 2014
- [46] B.L. van der Waerden, *Eine Bemerkung über die Unzelegbarkeit von Polynomen*, Math. Ann. 102 (1930) 738–739.
- [47] Zacharias G., *Generalized Gröbner bases in commutative polynomial rings*, Bachelor's thesis, M.I.T. (1978)